Chapitre I : L'approche globale d'Entreprise Risk management : Le carde conceptuel et méthodologique

L'entrée dans le XXIe siècle a mis en évidence l'importance des risques dans les sociétés modernes et dans les entreprises en particulier. Terrorisme, faillite de la gouvernance d'entreprise, développement du risque informationnel avec l'essor formidable d'Internet, obligent les entreprises à investir ou réinvestir de manière forte le champ de management du risque. Création d'une culture du risque, management participatif, système de catégorisation, mise en place de cellule de veille, les outils de management ne manquent pas pour comprendre et gérer les risques.

A ce titre, ce premier chapitre aborde les différents concepts liés au management du risque et à ses approches et cadre normatif. Il représente la revue de littérature sur laquelle nous nous somme basé afin de collecter les informations nécessaires à cette étude, elle est rédiger essentiellement des différents ouvrages et revues scientifiques. Ce chapitre est scindé en trois sections :

Pour la première section, un rappel historique permettra de comprendre l'apparition de la notion de risque, on découvrira ce concept à travers ses définitions en montrant ses typologies et l'acceptation du risque dans l'entreprise.

Dans la deuxième section, on montrera l'histoire de la pratique du risk management, on exposera les approches et le vocabulaire autour de ce terme, on citera ses finalités et objectifs, on métrera en évidence les normes et référentiels du risk management.

Et la dernière section s'appuie sur les grandes lignes directives portant sur l'intégration et l'implantation du cadre organisationnel de management du risque selon la norme ISO 31000, ainsi, d'autres référentiels tels que le cadre du COSO-II peuvent être utilisés pour enrichir l'objet de cette section.

Section 1: La complexité du risque dans l'entreprise

Bien que l'analyse des risques et leur mode de management soient au cœur de nombreux travaux de recherche, le risque demeure un concept difficile à définir. La littérature compte différentes typologies de risques, proposant des regroupements sous forme de familles de risques différenciés selon leur nature, leur origine, leurs effets, leurs conséquences, etc.

Dans cette section, nous aborderons les différentes définitions du risque, ses typologies ainsi que l'acceptation du risque dans l'entreprise.

1. La notion du risque : État des lieux des définitions

Les normes, les réglementations, les dictionnaires courants, etc., autant de sources pouvant présenter des définitions sensiblement différentes pour un même terme; chaque individu, ou groupe d'individus, peut déterminer une signification précise dans son champ d'application ou se faire inconsciemment sa propre représentation du terme.

Des nombreux auteurs s'intéressent à la notion de risque et à l'art et la manière de gérer ce dernier. Risques, danger, processus risqué, aléa, incidence, etc. ; il existe de nombreux termes et utilisations du mot risque, qu'il est difficile de distinguer.

Latin: Resecum, italienne: riscare, espagnole: risico[1]… Il est difficile d'établir avec exactitude l'origine du terme risque. Le sens qui lui est accordé s'est enrichi, développé au fil du temps et des cultures traversées. P-C. Pradier explique que, de nos jours, différents emplois du mot risque se côtoient : « on confond donc le risque avec sa mesure (métonymie) et avec ce qu'il menace [2]».

Face à cette variété de sources, de perceptions des conséquences ou même de domaines ou de cultures, une multitude de définitions ont été proposées : académiques (Courtot, 1998; Knight, 1921; Gourc, 2006), mais aussi de la part d'organisations telles que ISO, AFNOR, DGA, CIRANO, COSO, OGC… (DGA, 1995; AFNOR, 2003; CIRANO, 2003; Australian/ New Zealand Standard, 2004; International Organization for Standardization, 2008, 2009).

En effet, ce terme, en traversant les siècles, s'est changé de sémantiques (ou sens) différents. Qu'entend-on par risque ? Dans le langage courant, le terme risque est synonyme de danger, d'événement malheureux. Il désigne menace objective. De manière paradoxale, on peut dire que « rien n'est un risque » mais également que « tout peut être un risque » ; tout dépend de la manière dont on considère le danger ou l'événement avant le qualifier. Ainsi parle-t-on souvent de « prendre des risques » en s'intéressant à l'esprit d'entreprise. Il n'est plus question de danger car ici le risque décline avec la notion de chance, de hasard, de probabilité, d'éventualité d'une part mais d'autre part de perte et gain.il est plutôt question d'opportunités par opposition aux menaces.

Les travaux séminaux portant sur le calcul des probabilités remontent à Blaise Pascal et Pierre de Ferma au XVII^{e} siècle (1654). Il fallut attendre un siècle pour que Jacob Bernoulli formule la loi faible des grands nombres en 1713 et que Daniel Bernoulli introduise la notion d'utilité dans la théorie de la décision en avenir risqué. Ce n'est en sus qu'au XX^{e} siècle que John von Neumann et Oskar Morgenstern ont présenté une théorie unifiée de la décision en avenir incertain et de comportement face au risque. La théorie du risque comme nous l'entendons actuellement date du dernier siècle et a été complétée par les travaux de

[1] Xavier Michel, Patrice Cavaillé et Coll; Management des risques pour un développement durable: qualité, santé, sécurité, environnement; édition Dunod; Paris; 2009; p5.

[2] Guillaume Marques; Management des risques pour l'aide à la gestion de la collaboration au sein d'une chaîne logistique: une approche par simulation; thèse de doctorat de l'institut national Polytechnique de Toulouse INP; spécialité : systèmes industriels; Décembre 2010; p37.

Kahneman et Tversky. Raison pour laquelle en s'appuyant sur la théorie du risque, on ne s'assure que contre certains risques[1].

En 1921, Frank khigt[2] a proposé une dichotomie ou distinction de l'incertain en d'une part l'incertitude et d'autre part le risque. Une situation est réputée risquée s'il est possible d'affecter des probabilités objectives ou subjectives aux différents états possibles. Dans le cas contraire, on parlera d'incertitude. Néanmoins, les assureurs ne sont concernés que par l'incertain mesurable. C'est-à-dire par les situations relevant de divers scénarios probabilistes de réalisation. La connaissance de la distribution de probabilité du risque considéré permettra d'inférer sur la moyenne et la dispersion du risque*.

A ce propos, nous renvoyons vers les travaux d'A. Sienou (2009)[3] qui a dressé une liste plus exhaustive des définitions possibles du mot risque comme suit :

Tableau N°1: Différentes définitions du risque

Auteur	Définitions	Domaine
Markowitz, 1952	Variance of return	Finance
Marrs et Mundt, 1982	Business risk is the threat that an event or action will adversely affect an entity's ability to achieve its business objective and execute its strategies successfully	Management
Kervern et Rubise, 1991	Le risque est la mesure du danger.	industrie
IFRIMA, 1994	The compound estimate of the probable frequency, severity, and public perception of harm.	Assurance
IFRIMA ,1994	Possibility of loss or exposure to loss	Assurance
IFRIMA ,1994	Peril which may cause loss	Assurance
IFRIMA, 1994	Hazard or condition which increases the likely frequency or severity of loss.	Assurance
IFRIMA, 1994	Property or person exposed to loss	Assurance
IFRIMA, 1994	Potential dollar amount of loss.	Assurance
IFRIMA, 1994	Variations in actual losses.	Assurance
IFRIMA, 1994	Uncertainty concerning loss.	Assurance

[1] Octave Jokung Nguén; Management des risques; Edition Ellipses; Gestion; Paris; 2008; p11.
[2] http://fr.wikipedia.org/wiki/Risque
* La moyenne sera mesurée par l'espérance mathématique tandis que la dispersion résultera de la variance ou de manière équivalente de l'écart type.
[3] Amadou SIENOU ; Proposition d'un cadre méthodologique pour le management intégré des risques et des processus d'entreprise ; Thèse de doctorat en Systèmes Industriels ; Ecole Doctorale Systèmes Unité de recherche, Centre de Génie Industrie ; Mines Albi ; Université de Toulouse l'université de Toulouse ; Franc ; 26 Juin 2009.pp 42-43.

IFRIMA, 1994	Uncertainty or variation attached to the outcome of a given situation.	Assurance
IFRIMA, 1994	The uncertainty of attaining a standard.	Assurance
IFRIMA, 1994	The likelihood of a specified uncertain event occurring within a specified period or under specified circumstances.	Assurance
IFRIMA, 1994	The likelihood of something happening.	Assurance
Canadian Standards Association, 1997	The chance of injury or loss as defined as a measure of the probability and severity of an adverse effect to health, property, the environment or other things of value.	Management
Wybo, 1999	Un risqué est un aléa dont la survenance prive un système d'une ressource et l'empêche d'atteindre ses objectifs.	Industrie
Guide ISO/CEI 51, 1999	Combinaison de la probabilité d'occurrence d'un dommage et de sa gravité.	Ingénierie de systèmes
SAA/NZS HB 143, 1999	The chance of something happening that will have an impact on objectives.	Norme nat.
IEEE Standard 1540,2001	The likelihood of an event, hazard, threat or situation occurring and its undesirable consequences; a potential problem.	Ingénierie de systèmes
Treasury Board of Canada, 2001	Risk refers to the uncertainty that surrounds future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to influence the achievement of an organization's objectives.	Management
Kontio, 2001	A possibility of loss, the loss itself, or any characteristic, object, or action that is associated with that possibility.	Projet
ISO/IEC GUIDE 73, 2002	Combination of the probability of an event and its Consequence	Approche générale
NASA, 2002	The combination of (1) the probability … that a program or project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, compromise of security, or failure to achieve a needed technological breakthrough; and (2) the consequences, impact, or severity of the undesired event were it to occur.	Ingénierie de systèmes
Office of Government Commerce, 2003	Risks are things that may happen at some point in the future and require positive management to reduce their likelihood of happening, their impact on the programme, or both	Projet
ISO 17666, 2003	Undesirable situation or circumstance that has both a likelihood of occurring and a potential negative consequence on a project.	Projet

COSO, 2004	The possibility that an event will occur and adversely affect the achievement of objectives	Contôle interne
PMI, 2004	An uncertain event or condition that, if occurs, has a positive or negative effect on a project's objectives	Projet
AS/NZS 4360, 2004	The chance of something happening that will have an impact on objectives	Management
Zur Muehlen et Rosemann,2005	Risk describes the probability with which an error will lead to an (unwanted) consequence	Ingénierie de systèmes
Kerzner, 2005	Measure of the probability and consequence of not achieving a defined project goal	Projet
Office of Government Commerce, 2005	Uncertainty of outcome, whether positive opportunity or negative threat	Projet
DoD, 2006	A measure of future uncertainties in achieving program performance goals within defined cost and schedule constraints	Défense
Gourc, 2006	La possibilité que survienne un événement dont l'occurrence entraînerait des conséquences (positives ou négatives) sur le déroulement de l'activité du projet.	Projet
Alberts, 2006	Operational risk is the potential failure to achieve mission objectives.	Manag. des opérations
ISO 31000, Guide ISO/IEC 73, 2009*	Effect of uncertainty on objectives	Appr. globale

Source: Amadou SIENOU; 2009 ; op.cit ; pp 42-43.

Cet ensemble de définitions, confirme que le risque est un concept qui a plusieurs facettes selon les applications ou les contextes. Dont, la norme ISO 31000: 2009 - Management du risque - Principes et lignes directrices peut être considéré comme une référence couramment utilisée, elle définit le risque comme l'effet de l'incertitude sur l'atteinte des objectifs.

Cette nouvelle définition ne remet pas en cause les problématiques de traitement des dangers ou l'analyse des événements dommageables. Elle les complète en formalisant l'importance du rôle des décideurs[1].

Dans le cadre du vocabulaire proposé par le guide 73 ISO / IEC, 2009[2], l'effet est décrit comme un écart positif et/ou négatif par rapport à une attente. Ainsi, l'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un

* Cette définition provient du référence ISO Guide 73-Vocabulaire du management du risque- qui a été revu lors du développement de la norme ISO 31000: 2009- Management du risque-Principes et lignes directrices.

[1] Gilles Motet; Les cahiers de la sécurité industrielle; la norme ISO 31000; 10questions; FonCSI; 2009;p3.

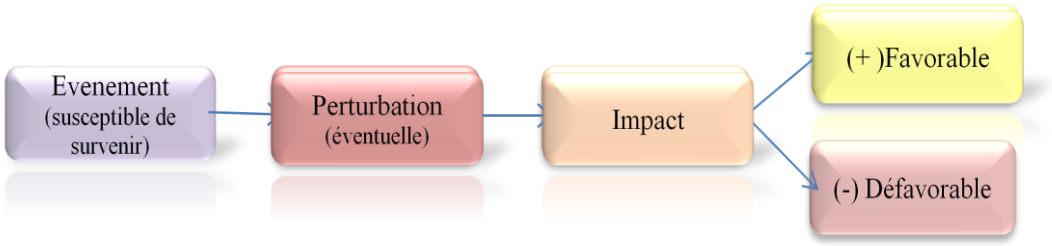
[2] ISO/IEC guide 73; Risk management-Vocabulary; Geneva; ISO; 2009; p1.

événement, de ses conséquences ou de sa vraisemblance. Cette dernière est la possibilité que quelque chose se produise.

Pour un souci de compréhension du vocabulaire autour du risque, nous mettons l'accent sur les interprétations évoquées par D. Gourc, dont, il décrit le risque[1] par un triplet ″Occurrence, Effet, État″ ; l'occurrence permet de caractériser le risque par son identité, ses origines et les chances de survenue. Ainsi les types et la mesure des niveaux d'impacts correspondent à l'effet, tandis que l'état permet de décrire la nature évolutive du risque en relation au temps, hasard et incertitude.

Dans une perspective de gestion du projet, Gourc définit le risques comme une possibilité que survienne un événement dont l'occurrence entraînerait des conséquences positives ou négatives sur le déroulement de l'acticité du projet ou la performance du système en général.

Figure N°1 : Le modèle général du risque selon Gourc



Source : D.Gourc, Op.cit ; p 31.

Comme l'illustre la figure 1, le risque dépasse le simple événement. Il apparaît comme une notion dynamique qui se matérialise autour de quatre éléments fondamentaux. Étant donnée une circonstance normale, un événement potentiel ou probable peut causer une perturbation éventuelle* (une situation perturbée). Cette perturbation influence les indicateurs de performance ou critère du succès du projet. L'impact, favorable ou défavorable, constitue une « mesure qui définit l'importance des perturbations occasionnées par l'occurrence du risque ».

Le croisement d'un événement et d'une situation sera appelé source de risque. Ici, la notion de situation englobera le contexte des facteurs de risque. Ils peuvent être décrits comme des éléments identifiés ou une condition de l'environnement interne ou externe dont l'existence est de nature à influencer la survenue d'un événement. En plus de l'occurrence de l'événement, le facteur peut également influer sur l'importance de sa conséquence.

Nous constatons que le risque est un concept multi dimensionnel associé essentiellement aux dimensions « occurrence et effet », dont gravité mesure l'importance des effets qu'il induit. Ces deux dimensions, complétées par la détectabilité, définie comme la capacité de apercevoir le phénomène, entrent dans la qualification d'une caractéristique globale du risque « la criticité».

Le concept de risque ne peut être également dissocié de l'idée de partie prenante. Au delà du fait avéré, dans le risque, tout est perception. De la caractérisation de l'occurrence à l'évaluation des conséquences (l'attente, l'objectif), la mesure du risque ne peut être dissociée du regard porté sur lui par l'homme. De nombreux facteurs influencent cette perception du

[1] Didier Gourc; Vers un modèle général du risque pour le pilotage et la conduite des activités de biens et de services : Propositions pour une conduite des projets et une gestion des risques intégrées; Thèse de HDR; École des Mines d'Albi-Carmaux; Institut national polytechnique de Toulouse; 2006; pp 29-30.

*L'existence d'un référentiel (planning d'événement, budget, performance attendus) permet d'identifier les perturbations occasionnées par l'occurrence de l'événement.

risque: phénomènes culturels, aversion au risque, nombre d'expériences antérieures similaires…Le risque est donc éminemment subjectif et associé à une perception de l'acteur humain ou le décideur.

D'ailleurs, il est intéressant de remarquer que dans cette vision le décideur ne « subit » pas le risque mais le « prend ». Cette prise de risque s'appuie donc sur une logique, une démarche intellectuelle, précise et justifiée. A partir de cette prise de conscience, le risque peut s'inscrire dans une démarche « raisonnée et mesurée » afin d'en contrôler les effets au travers de certaines décisions. Deux attitudes peuvent exister alors. Le décideur peut alors entrer dans une recherche d'opportunités où le risque peux prendre une forme positive puisque vecteur potentiel de création d'une quelconque valeur. Inversement, adoptant une vision négative (plus traditionnelle) des conséquences possibles d'un événement sur un système (système naturel, entreprise, projet, groupe d'hommes,…), la cyndinique, ou science du danger, se proposent d'étudier les sources, les caractéristiques et les conséquences de ces Événement Non Souhaités (ENS).

Au final, contrôlable ou non, positif ou négatif, le risque est donc également multiforme et sa prise en compte passe par une démarche intellectuelle plus ou moins formalisée et formalisable, nous discuterons plus loin de ces concepts.

2. Typologies du risque d'entreprise

Les entreprises encourent des risques divers et variés dés leur création et au cours de leur existence. Ces risques sont relatifs à l'activité et à la localisation d'entreprise. L'enjeu pour elle est par conséquent sa survie par la création de valeur afin de satisfaire ses différentes parties prenantes ou stakeholders que sont les clients, les fournisseurs, les employés, les créanciers, les managers et la communauté dans la quelle l'entreprise évolue.

Ce faisant la valeur de l'entreprise résultera de la confrontation des choix stratégiques ou des décisions, en l'occurrence les risques acceptés et pris volontairement, et des conséquences négatives des risques subis par l'entreprise. On peut classifier les Risques d'entreprise et les différencier selon leur nature, origine ou domaine d'activité.

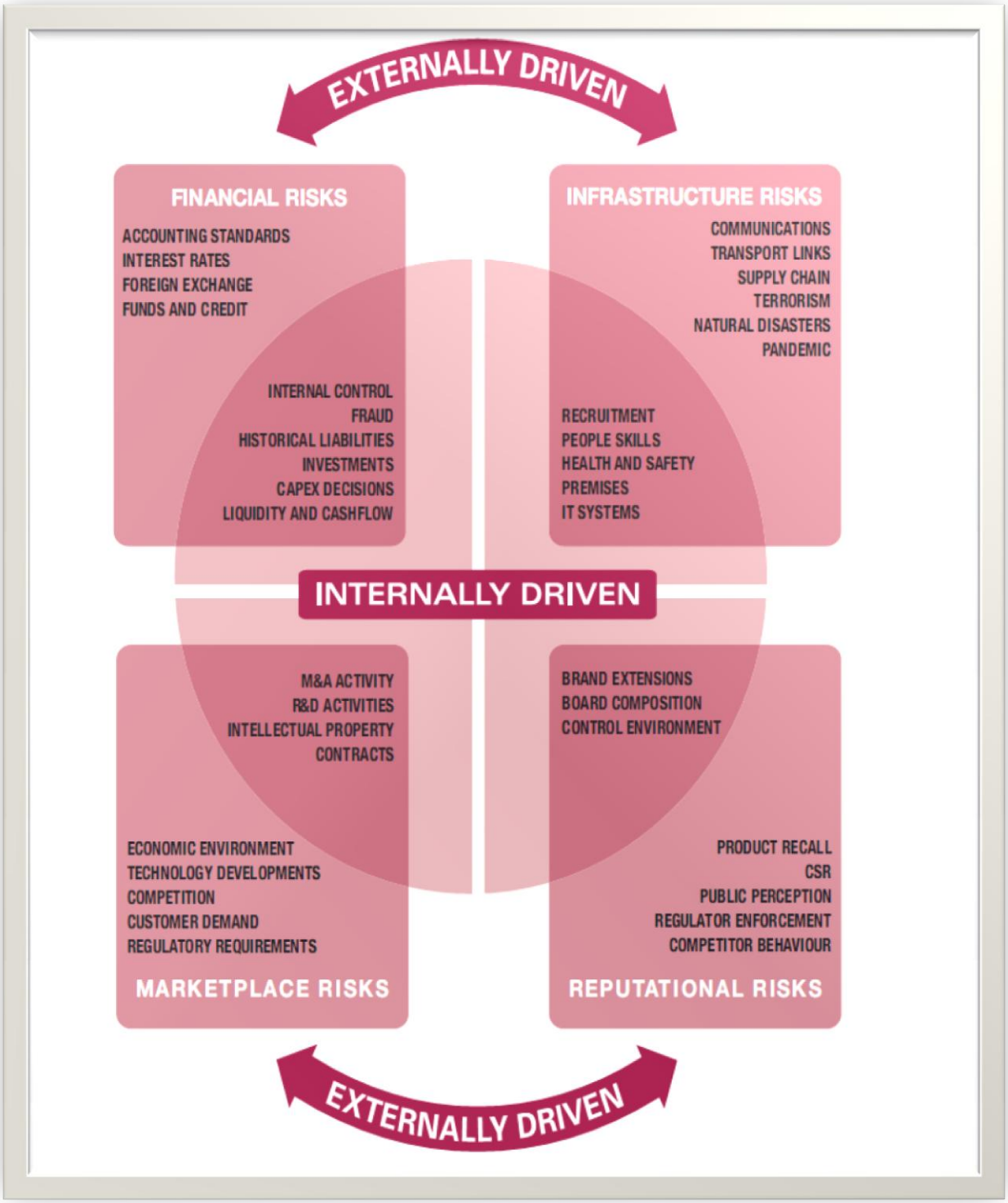
2.1. Les risques différenciés par origine

Aujourd'hui, l'entreprise évolue dans un environnement vaste, complexe et dynamique, source de multiples facteurs aggravants pour les risques d'entreprise. Et pour que l'entreprise évoluer, elle devra à la fois être attractive (présenter de produits/ services satisfaisants aux meilleurs prix et qualité, attirer des investisseurs, des compétences…), compétitive (dégager des bénéfices…) tout en prenant rationnellement les risques en trouvant les compromis nécessaires. Dont, l'origine des risques peut être interne ou externe à l'entreprise.

Dans ce contexte, FIRM[1] Risk Scorecard risk propose une classification des risques illustrée ci-dessous :

[1] A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 ; AIRMIC; Alarm, IRM; 2010; p14.

Figure N°2 : Les facteurs des risques internes et externes de l'entreprise selon FIRM

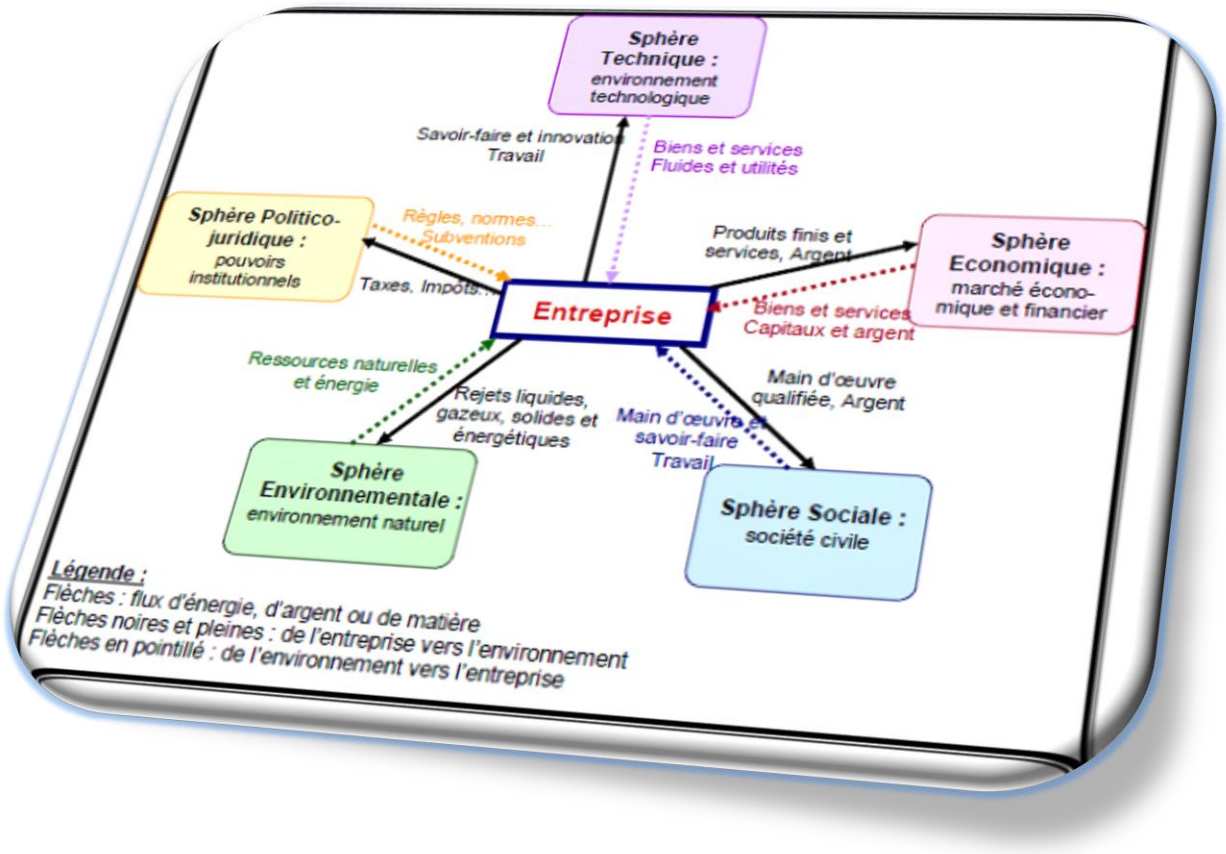


Source: AIRMIC, Alarm, IRM; Op.cit; p14.

La figure présentée plus haut montre que certains risques répondent à des facteurs à la fois internes et externes, de ce fait ces zones se recoupent. Le classement des risques peut être affiné en distinguant par exemples des risques d'ordre stratégique, financier, opérationnel et cetera.

L'environnement externe de l'entreprise est varié car composé d'éléments économiques, sociaux, politiques, naturels, etc. afin d'avoir une vision claire des éléments et des contraintes avec lesquels l'entreprise interagit, il est pertinent de modéliser l'environnement de l'entreprise selon les cinq sphères illustrées dans la figure ci-dessous[1] :

Figure N°3 : Modèle externe de l'entreprise



Source: A DASSENS et autres; Une approche globale de l'analyse de risques en entreprise; 2005;p5.

Comme nous venons de démontrer, les cinq sphères sont :

- Sphère technique (environnement technologique) comprend les infrastructures, les industries, les voies de communication et aussi les ressources techniques comme les matières premières, les matériels disponibles, les innovations technologiques, etc.
- Sphère économique (marché économique et financier) composée des différents acteurs économiques, les clients, les fournisseurs, les distributeurs, les sous-traitants, et financiers comme les actionnaires, les banques, les assureurs qui disposent des ressources économiques et financières nécessaires au fonctionnement de l'entreprise.

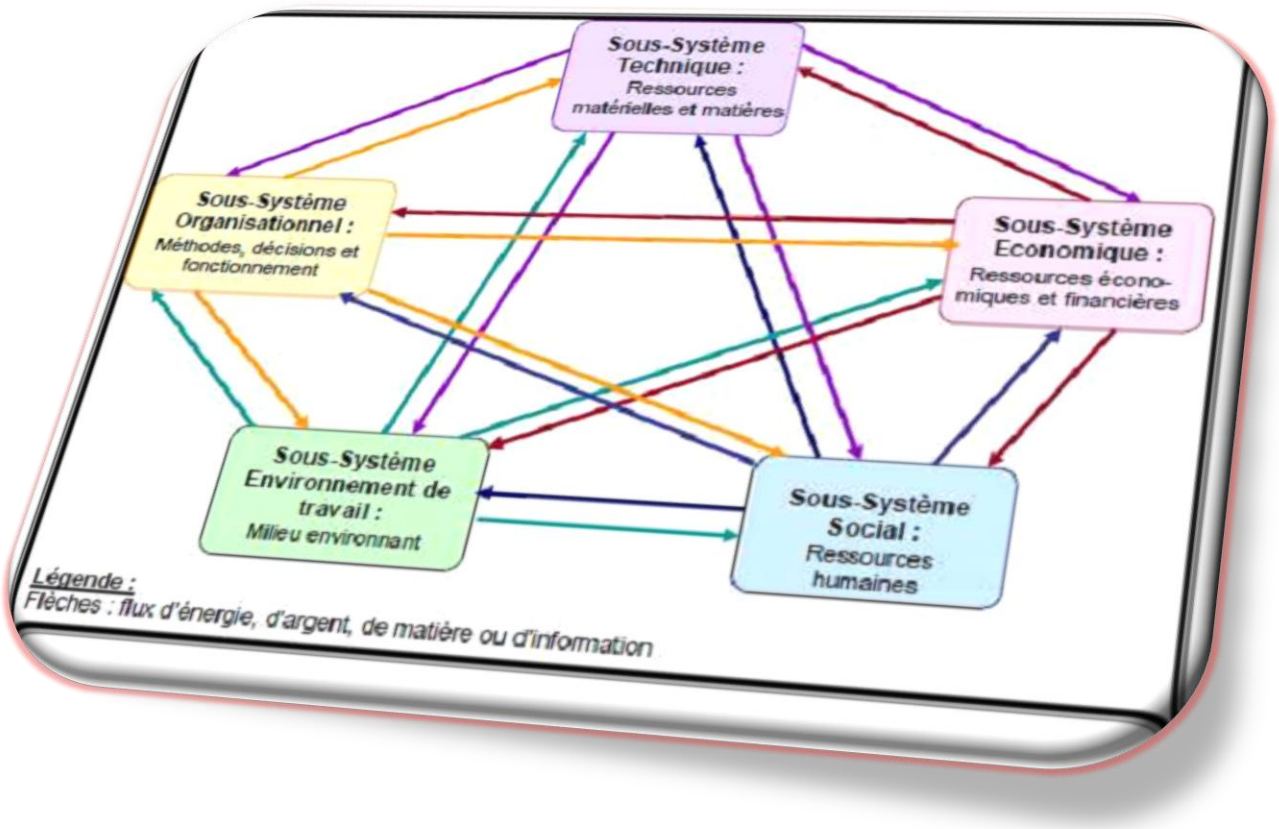
[1] Audrey DASSENS, Jean-François BRILHAC, Patrick ROUSSEAUX, Richard LAUNAY; Une approche globale de l'analyse de risques en entreprise; 6ème Congrès Européen de Science des Systèmes; de 19 au 22 septembre 2005; p5.

- Sphères politico-juridique (pouvoirs institutionnels) comme l'État, les collectivités territoriales, les instances de contrôles qui sont sources de lois, normes, réglementations, injonctions, etc. elle est également composée du contexte professionnel de l'entreprise comme l'holding, les branches professionnelles à l'origine de certaines valeurs et normes.
- Sphère sociale (société civile) comprend les associations, les syndicats, etc. Qui représentent notamment les réservoirs de savoir-faire et de main d'œuvre pour l'entreprise.
- Sphère environnementale liée à l'environnement physique (l'eau, l'air, sol), biologique avec l'ensemble du monde vivant et l'environnement météo-logique (le vent, la température).

Ainsi, on peut démontrer l'environnement interne de l'entreprise selon cinq sous-systèmes de l'entreprise suivants[1] :

- Sous-système technique (ressources matérielles et matières)
- Sous-système économique (ressources économiques et financières)
- Sous-système organisationnel (stratégies, processus décisionnels et fonctionnels, communication, règles et procédures, organigramme, etc.)
- Sous-système social (ressources humaines)
- Sous-système environnement de travail (la condition de travail)

Figure N°4 : Modèle interne de l'entreprise



Source: Elena Loredana Podea, Op.cit; p 33.

[1] Elena Loredana Podea; Cartographie des situations à risque dans les projets de conception de produits innovants pour l'aide à la décision; thèse doctorat en cotutelle entre l'université Bordeaux1 " École doctorale des sciences physiques et de l'ingénieur" et l'université Polytechnique Bucarest; Spécialité: Productique; Septembre 2009; pp 30-31.

Les différents volets de l'environnement soit externe ou interne de l'entreprise nous permet de visualiser non seulement des exigences relatives aux clients, aux marchés, aux fournisseurs, mais également celle relatives à la société dans son ensemble. Parmi ces dernières, les questions d'environnement autant par l'intermédiaire des exigences réglementaires que par la pression des clients, des associations ou des élus ou par celle du marché à travers le coût de matières premières comme des traitements des effluents et des déchets. Ainsi des exigences liées aux risques de santé et sécurité au travail. Les enjeux internes seront essentiels à une bonne prise en compte des exigences externe dans les relations de l'entreprise.[1]

2.2. Les risques différenciés par nature :

De nombreuses distinctions ont été proposées pour caractériser les différentes natures de risque auxquels peuvent être soumis les entreprises. Nous en retiendrons trois.

⌖ risques purs versus risques spéculatifs[2]

En 1978, M. HALLER présente un découpage structurel du risque basé sur l'espérance de gain dissociant les classes de "Pur Risk" et "Speculative Risk". Ainsi en 1981, dans leur ouvrage "Gestion des Assurances de l'entreprise", M. SALVADOR et P. GONDE donnent une définition plus complète des risques purs et spéculatifs, en tentant de les caractériser.

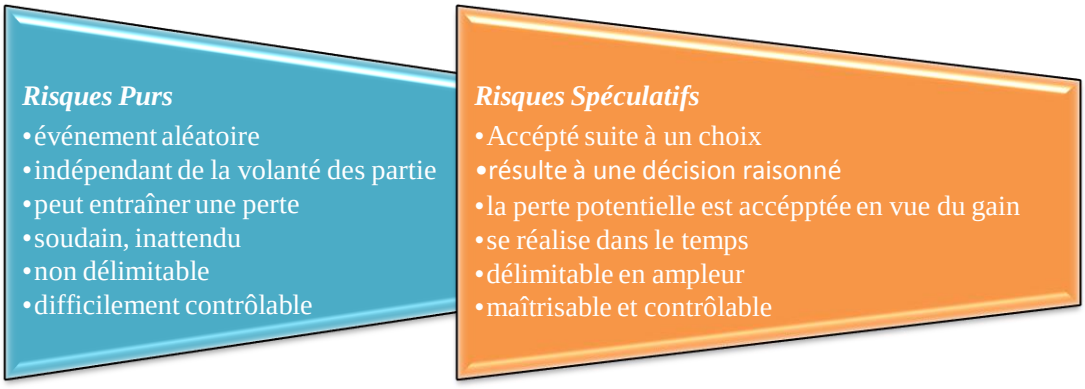
En 1993, une étude menée par une société de conseil spécialisée dans la gestion des risques SAGERI auprès d'une quarantaine de sociétés françaises et européennes montre que la distinction entre risques purs (risques accidentels et aléatoires) et risques spéculatifs apparaît dans certaines entreprises.

Un risque est spéculatif ou « risque-action » lorsqu'il présente une chance de gain et une chance de perte. Le risque spéculatif, ou risque d'entreprendre, est défini comme le fruit d'une décision de gestion ou un choix stratégique qui est prise dans le but d'accroître des profits, mais qui comporte des risques de pertes.

Le risque pur ou « risque-écueil » est indépendant de la volonté du décideur. Il résulte de la manifestation d'événements non souhaités naturels ou fortuits. Le risque pur se situe à l'opposé du risque spéculatif et ne présente qu'une chance de perte.

Le tableau suivant présente les principales différences entre les risques purs et spéculatifs.

Figure N°5 : Risques purs versus risques spéculatifs



Source : Marc Fumey; Op.cit; p39.

[1] Xavier Michel, Patrice Cavaillé et Coll; Op.cit; p31.
[2] Marc Fumey; Méthode d'évaluation des risques agrégés : application au choix des investissements de renouvellement d'installations; thèse de doctorat en systèmes d'industriels; l'institut national polytechnique de Toulouse; Janvier 2001; pp38-39.

En 1989, C. MARMUSE souligne que "l'économie classique a souvent opposé ces deux types de risques en les dissociant. Seul le risque spéculatif intéresse véritablement le management, le risque pur étant considéré comme ne relevant que du hasard ou de l'infortune". Aujourd'hui, la réalité est autre, la vulnérabilité des entreprises conduit le management vers une gestion intégrée de ces deux risques.

Le risque inhérent versus le risque résiduel

Le risque inhérent est le risque pur ou brut, considéré sans les éventuels moyens de protection ou de contrôle mis en place[1].Par contre le risque résiduel est lié au contrôle, en raison des limitations ou de maîtrise inhérent au contrôle interne d'entreprise ou de l'organisation[2].

Cependant, cette distinction est très importante car elle permet de valoriser la pertinence des actions de la maitrise ou de traitement du risque.

Les risques majeurs

Nous en dénombrerons principales aux risques naturels, risques technologiques, incluant les risques de transport et les risques sanitaires, et les risques diffus ou risques de la vie quotidienne. Le risque majeur ou risque collectif se caractérise par une faible fréquence et une forte gravité. Ainsi, les risques liés aux conflits armés, que nous n'abordons pas, sont également caractérisés de la sorte et peuvent donc être assimilés aux risques majeurs.

Ce fait a des conséquences tout à fait majeures, plus on s'éloigne du domaine de fonctionnement normal, pour aller vers l'incident ou l'accident, plus la perception de la gravité se détériore. Autrement dit, plus la situation est grave, complexe, mal reconnue, peu fréquente[3].

2.3. Les risques différenciés par domaine d'activité

La nature des risques est différente selon le domaine d'activité de l'entreprise. Le risque peut donc être différencié selon qu'il concerne les produits de l'entreprise, les projets de l'entreprise ou l'entreprise elle-même.

Dans ce contexte Desroches[4] classe ces risques quelque soit son niveau (entreprise, projet ou produit) comme suit :

✓ Pour l'entreprise, les risques peuvent apparaître comme étant :

1- Les risques politiques
2- Les risques programmatiques
3- Les risques stratégiques
4- Les risques techniques
5- Les risques opérationnels
6- Les risques juridiques
7- Les risques financiers
8- les risques économiques
9- Les risques commerciaux
10- Les risques de communication
11- Les risques professionnels
12- Les risques des systèmes d'information
13- Les risques sociaux
14- Les risques de management et d'organisation
15- Les risques d'insécurité
16- Et d'environnements naturels et technologiques

[1] Boukhechba Mohamed Sami; La cartographie des risques opérationnels : la CNEP Banque; mémoire de fin d'étude; École Supérieure de Banque; Octobre 2007; p20.
[2] Mohamed Hamzaoui, Benoît Pigé; Audit: gestion des risques d'entreprise et contrôle interne, Norme ISA 200, 315, 330, 500; Pearson Éducation; France; 2005; p173.
[3] Yves Métayer, Laurence Hirsch; Premier pas dans le management des risques; Edition AFNOR;2007; P21.
[4] Desroches; les invariants de l'analyse préliminaire des risques; Qualita 2005; 6 éme Congrès International Pluridisciplinaire; Qualité et Sûreté de Fonctionnement; Actes du Congrès; Vol 2; Bordeaux; du 16 au 18 mars 2005, p 687-688.

Par exemple, un facteur de risque politique à considérer est l'application d'une nouvelle législation nationale ou européenne. De même un facteur de risque stratégique à prendre en compte est l'instabilité des besoins ou du contexte économique ou politique.

✓ ***Les risques projets :***

L'AFITEP et AFNOR[1] définissent le risque projet comme étant "la possibilité qu'un projet ne s'exécute pas conformément aux prévisions de date d'achèvement, de coût et de spécifications, ces écarts par rapport aux prévisions étant considérés comme difficilement acceptables voire inacceptables". Cette définition s'attache essentiellement à la mesure des conséquences du risque projet sur les critères de délais, de coût, performance et qualité; nous rajoutons le critère d'image de projet et le degré de satisfaction, etc. susceptible de survenir à différentes étapes de la réalisation du projet.

Lors, les risques consistent :

1- Risques d'expression des besoins et de spécifications
2- Risques de stratégie de développement
3- Risques d'organisation de Projet
4- Risques d'Interfaces contractuelles
5- Risques de conduite de projet
6- Risques financiers du projet
7- Risques de retards de planning
8- Risques sur les performances techniques et opérationnelles
9- Risques des utilisateurs et sites d'exploitation

Par exemple un facteur de risque d'expression des besoins et de spécifications est la non implication, même limitée des futurs utilisateurs dans la définition du besoin. De même, un facteur de risque d'organisation du projet est l'absence d'ingénieur système.

✓ ***Les risques produits***

Les risques liés aux produits utilisés ou commercialisés par l'entreprise peuvent être l'échec commercial (mauvaise qualité, quantité insuffisante, etc.), la non conformité d'un produit ou encore sa dangerosité.

Considérant uniquement les produits utilisés dans l'entreprise, les risques produits sont d'abord ceux qui relèvent de la sûreté de fonctionnement du produit; ils touchent les utilisateurs du produit et son environnement.

Par exemple un facteur de risque en conception et fabrication est la non prise en compte des causes communes de défaillance…, De même, un facteur à risque d'exploitation est l'absence ou la mauvaise compréhension des procédures de maintenance

3. L'acceptabilité du risque d'entreprise

Les recherches et les travaux étudiés lors de la revue de littérature font, pour la majorité, référence aux éléments clés de la notion du risque, soit l'acceptation du risque qui s'articule autour et la perception du risque, l'attitude face au risque ainsi la criticité.

La norme ISO (guide ISO/CEI 73: 2009) stipule que l'acceptation du risque est une décision argumentée en faveur de la prise d'un risque particulier où l'admission un avantage potentiel d'un gain ou de perte dépend des critères du risque retenus par la personne qui prend la décision. Soulever

3.1.Perception et attitude face au risque

Selon ISO (guide ISO/CEI 73: 2009), la perception du risques est définit étant qu'un ensemble de valeurs ou préoccupations aux travers desquelles une personne, un groupe ou un organisme considère un risque.

[1] AFITEP, AFNOR ; Dictionnaire de management de projet; ouvrage collectif; 2000. http://www.afitep.fr

A ce propos, nous renvoyons vers l'article [1] de Caroline Aubry, qui soulève que la notion de risque perçu nous fait passer d'une approche rationnelle et non-interprétative du risque qui est celle des experts à une approche subjective qui est celle des individus. En effet, la prise en compte de la dimension subjective du risque complique son évaluation mais elle est particulièrement intéressante dans la mesure où elle permet de mettre en évidence le rôle des biais cognitifs et des représentations dans l'appréhension et l'évaluation des risques par les acteurs économiques.

Caroline rajoute que la perception du risque est ainsi fortement liée et influencée aux caractéristiques individuelles, en particulier à la personnalité de l'acteur, leur appétit ou goût du risque, à son vécu intérieur et antérieur, à ses préjugés et à sa sensation de perte ou de gain potentiel face à une situation.

Cependant, l'attitude face au risque est un état d'esprit conscient, une vue mentale ou disposition vis-à-vis d'un fait ou d'une incertitude, ou simplement une réponse consciente à la perception d'une incertitude significative[2].

L'attitude face au risque est généralement appréhendée par le biais de trois concepts, en l'occurrence l'aversion vis-à-vis du risque, la prudence et la tempérance[3] :

- **L'aversion du risque**, correspond à la concavité de la fonction d'utilité. En effet, une fonction d'utilité concave renvoie à la volante d'un individu de se débarrasser du risque. Elle traduit également ce que les économistes appellent le principe de l'utilité marginale décroissante[*]. Cet état implique une asymétrie dans la perception des gains et des pertes, dont les pertes en réduisant la richesse, affectent plus l'utilité que les gains identiques qui augmentent la richesse. Notant que, l'aversion ne signifie pas que l'on ne prend pas le risque, mais plutôt que l'on n'est prêt à payer un certain prix pour en être débarrassé.
- **La prudence**, ne mesure pas la volanté d'être débarrassé d'un risque mais la propension à se préparer pour faire face au risque. Ce concept est directement raccordé à la convexité de l'utilité marginale. Bien entendu, un individu peut être prudent et aime le risque ou bien d'être prudent et déteste le risque. Avec la prudence, on s'intéresse aux effets marginaux du risque et non plus à son impact global comme c'était le cas avec l'aversion.
- Le dernier concept, celui de **tempérance** (tolérance, neutralité), est utilisé lorsque les individus font face à plusieurs sources de risques. La tempérance ne dépend ni de la prudence ni de celui d'aversion, mais elle est à la prudence ce que la prudence est à l'aversion. En effet, le décideur peut être tempéré, prudent et amoureux du risque. En sens économique, la tempérance se trouve au niveau de concavité de la dérivée seconde de la fonction d'utilité.

En quelque sorte, on peut distinguer deux catégories d'individus, comme Kahneman et Tversky montrent que les individus sont riscophiles[**], lorsque les conséquences des risques sont faibles, mais pour les conséquences importantes ces mêmes individus reviennent des riscophobes. Ce qui au niveau de leur d'utilité indique que la fonction croissante et convexe pour les faibles revenus suivie d'une fonction croissante et concave pour les revenus importants.

[1] Caroline Aubry; La gestion des risques dans les entreprises françaises: état des lieux et émergence d'une approche cognitive et organisationnel; revue Comptabilité et connaissance; France; 2007; p4.
[2] Elena Loredana Podea; op.cit; p 36.
[3] Octave Jokung Nguén; op.cit; pp 73-74.

[*] C'est-à-dire le fait que les accroissements de richesse successifs apportent de moins en moins d'utilité aux individus.

[**] Riscophiles : l'individu aime le risque. Riscophobes : l'individu déteste le risque.

Il est nécessaire de citer que le degré d'aversion vis-à-vis le risque influera plus la limite d'acceptabilité des risques. En fait, plus les décideurs seront frileux, plus la limite d'acceptabilité sera basse. Nous discuterons plus loin de ces concepts.

3.2.La criticité des risques

Nous captivons à la définition relevée par Helène Löning et d'autres auteurs[1], dons ils soulèvent l'acceptabilité d'un risque comme un niveau de criticité résultant d'une décision explicite et justifiée, fondée sur la gravité acceptée des conséquences.

Donc, la criticité est un concept couplé à l'attitude des décideurs vis-à-vis le risque, détermine la limite de leur acceptabilité.

Cet indicateur « criticité » cristallisera les deux dimensions caractéristiques du risque, la gravité et la survenance du risque. En effet, la criticité permet de valoriser et positionner les zones de risque selon leur importance comme on le verra plus détail par la suite.

La gravité est l'effet produit par la réalisation du risque, c'est-à-dire les impacts ou les conséquences que le risque peut avoir sur le respect des objectifs d'entreprise.

La survenance d'un risque est le rapport entre la probabilité d'occurrence (fréquence d'apparition par rapport au nombre de cas) et l'impact (coût des dommages et de remise en état) sur la bonne marche d'entreprise. La probabilité d'occurrence correspond aux chances raisonnables (à la vraisemblance mathématique) que le risque a de se réaliser lors du déroulement des activités d'entreprise et de se matérialiser en difficultés réelles. Le risque acceptable est fonction de l'impact probable et de sa gravité.

[1] Hélène Löning, Véronique Malleret, Jérôme Méric, Yvon Pesqueux, Ève Chiapello, Daniel Michel, Andreù Solé; Le contrôle de gestion : organisation, outils et pratiques; 3ème édition; DUNOD; Paris; 2008; p 244.

Section 2: Les fondements d'entreprise risk management : Une approche globale intégrée

Le risk-management comme on a vue précédemment est un processus d'identifier et de quantifier les risques qui peuvent affecter la réalisation des objectifs, et de proposer des stratégies pour traiter les risques, donc le risk-management apparait à la fois comme la raison d'être et la condition d'un contrôle interne adapté.

Afin de comprendre son évolution, il est indispensable de disposer de certains repères historiques, de montrer les approches qu'ils l'entourent en exposant ses finalités et ses objectifs et de mettre en évidence le cadre normatif et référentiel du risk management.

1. Entreprise Risk management : Le contexte général

Avant de plonger dans le vif du sujet, récapitulons un peu et penchons-nous sur un bref aperçu historique de l'apparition du risk management.

1.1. L'histoire de la pensé et la pratique du risk management

Les prémices du Risk Management appariassent au siècle des lumières lorsque le danger devient un objet de connaissance et non seul fait de forces étranges inconnues de l'homme. Mais ce n'est qu'un à deux siècles plus tard, que l'homme, porte par le développement des sciences, des techniques, des industries et face à leurs conséquences financières, humaines et environnementales, va réellement commencer à percevoir le risque comme un objet d'étude en vue de sa maîtrise. En effet, après la révolution industrielle, le siècle dernier a été marqué par des transformations fondamentales. Leurs éléments déclencheurs, exogènes aux entreprises, ont provoqué des réactions d'adaptation et la maîtrise des risques a dès lors pris une part croissante aux du fonctionnement et des résultats des entreprises[1].

Le risk management constitue une démarche d'analyse et d'identification systématique relativement récente dans le monde économique, mise à part certains secteurs historiques comme l'industrie maritime, nucléaire, pétrolière, chimique ou l'aviation...mais cela n'élimine pas totalement le risque! Le risk management est également particulièrement développé dans le domaine de la santé, et plus précisément dans les établissements de santé, publics ou privés, où le risk management et des vigilances sanitaires est devenue indissociable de la démarche qualité[2].

Dont, le risque est inhérent à l'entreprise. Il a toujours existé et constitue, d'après les économistes, son essence; Créer une entreprise, c'est déjà prendre un risque, sa survie n'est jamais assurée. Même les entreprises de grande taille n'ont aucune garantie de pérennité. Enron, Arthur-Andersen, Alstom et Parmalat sont des exemples des multinationales qui ont disparu ou qui ont dû lutter pour leur survie[3].L'activité entrepreneuriale est à la base une activité risquée et d'autres risques sont venus se greffer. Aux États-Unis, Henri Fayol, chef d'entreprise et ingénieur civil des Mines, voyait déjà en 1916 dans les « opérations de sécurité» visant la protection des biens et des personnes, l'une des six fonctions de «l'Administration ». Ainsi, il avait clairement déjà reconnu le « directeur sécurité stratégie ».

D'ailleurs, il est intéressent de passer par un bref historique d'évolution du risk management[4]; l'une des premières apparitions du concept de Risk management remonte à 1956 aux États-Unis, dans la Harvard Business Review, sous la plume de Russel Gallagher, responsable des assurances de la société Philico de Philadelphie. Il préconisait notamment d'employer une personne dédiée à temps plein pour gérer les risques et minimiser les pertes.

[1] Catherine Véret et Richard Mekouar; Fonction : Risk manager; Edition Dunod; Paris; 2005; p 22.
[2] Dossier sur le Risk Management publié par le groupe Effisoft; Février 2007; p5. www.effisoft.com
[3] Olivier Hassid; La gestion des risques; 2e édition; Dunod; Paris; 2008; p 5.
[4] Catherine Véret et Richard Mekouar ; op.cit; p27.

Dans les années 1970 à Philadelphie, sont diffusés les premiers écrits sur les fondements de risk management, notamment le manuel de George L. Head de l'Insurance Institute of America. Ainsi, le diplôme international « Associate in Risk Management-ARM » est délivré pour la première fois en 1973.

En 1975, l'association des acheteurs d'assurances professionnels américains change de nom afin d'intégrer la notion de risque, c'est le début du « Risk and Assurance Management Society-RIMS ».

En France, la prise en compte de cette notion au sein de l'entreprise apparaît plus tardivement. Même dans les années 1970, cette fonction est peu développée et structurée. Tandis que les publications et les colloques débuteront au début des années 1980; particulièrement avec les écrits de Patrick Lagadec et son concept de risque technologique majeur.

En 1988, société d'informatique Américaine rebaptise son service assurance en « service de gestion des risques » ; l'objet était de minimiser les ressources consacrées à la gestion des assurances et de réduire les effectifs ainsi d'externaliser les questions d'assurance.

En 1990, une grande société de téléphonie française se destine d'un service de gestion des risques en fusionnant les fonctions de protection de l'environnement et contrôle des pertes.

Puis, en 1991, Georges-Yves Kervern et Patrick Rubise diffusent L'archipel du danger, premier livre de référence sur les « sciences du danger » consacrant le terme de « cindyniques ». Les premiers colloques de cindynique, de violence urbaine, de thérapie familiale et de santé, se multiplient d'abord à la Sorbonne en 1994, puis au niveau européen.

À la fin des années 1990, les entreprises américaines, asiatiques, européennes et même africaines font face à la montée en puissance des risques politiques, économiques, socioculturels et technologiques ainsi l'émergence de nouveaux risques qu'une décennie plus tôt, tels que le développement de la cybercriminalité, l'insécurité dans les entreprises ou encore la mauvaise santé de leur personnel. En effet, les entreprises ont confrontées aussi d'une part à des risques physiques et moraux, et d'autres parts à des risques informationnels[1].

Dans cette époque, fin des années1990 et début des années 2000, connaître un foisonnement d'ouvrages théoriques et démarches pratiques, de réflexions internationales sur le thème des risques, des catastrophes, des crises et de leur maîtrise. Dont, le Risk management a pris une importance capitale dans la vie d'entreprise et commence à déboucher sur une vision plus globale et plus anticipatrice de toutes les vulnérabilités pouvant entraver la bonne marche de l'entreprise. Il tend à être intégré dans la stratégie globale d'entreprise et devient un élément qui peut influer sur les principes d'organisation.

Rappelant, Le 11 septembre 2001, les attentats du World Trade Center à New York ont un impact majeur sur l'économie américaine et sur nombreuses entreprises. Cette catastrophe a mis en exergue la fragilité des entreprises vis-à-vis de risques qui n'avaient jamais été envisagés et menée la nécessite d'une réflexion globale sur les risques.

Le 21 septembre 2001, l'explosion de l'usine AZF à Toulouse a conduit les entreprises à s'interroger sur la nécessité de communiquer sur les risques et de mieux prendre en compte les risques technologiques.

En décembre 2001, Enron, société américaine de distribution d'énergie, fait faillite en raison des pertes occasionnées par des opérations spéculatives maquillées en bénéfices via des manipulations des comptes malgré certifiés par le cabinet d'audit Arthur Andersen. Moins d'un an plus tard, durant l'été 2002 la société de

[1] Olivier Hassid ; Op.cit; p14.

télécommunications américaine Worldcom dépose son dossier de faillite à la suite de manipulations comptables . Ces deux scandales ont amenés les pouvoirs publics américains à légiférer sur la communication en matière de trésorerie, sur l'approche processus ainsi l'approche risque des entreprises.

Ce sont ces quatre évènements mondiaux majeurs qui marquent la prise de conscience des entreprises de leur fragilité vis-à-vis des risques : en premier lieu de leur vulnérabilité, en second lieu de leur carence dans la gestion de ces vulnérabilités et enfin de la nécessité d'intégrer le management du risque dans leur stratégie[1].

1.2. Grille de lecture des approches et vocabulaire autour le Risk management

Comme nous l'avons montré, les entreprises sont confrontées de plus en plus à une multitude de risque de nature différente. Dont, elles sont aujourd'hui progressivement devenues plus sensibles à la nécessité du management efficace des risques. Ainsi, il ne peut y avoir de politique de management du risque sans une connaissance précise des objectifs et orientations générales de l'entreprise; en effet, ces derniers constituant les référentiels de la prise en compte des risques. A ce titre, le management du risque peut se définir en termes d'objectifs ciblés (tactiques, opérationnels ou stratégiques); de contraintes à respecter (sociale, économique, réglementaire, juridique, etc.); de moyens techniques, humains et financiers à engager; de stratégie de traitement à privilégier (choix d'investissements, assurances, etc.) ; de priorités inter-domaines ou intra-domaines, etc[2].

Les banques croient qu'elles ont inventé le management du risque comme antidote à l'activité débridée de leurs pupitres de négociation. Pour leur part, les assureurs considèrent le management du risque comme leur droit sacré, mais les souscripteurs et les actuaires, dont la fragile entente caractérise le secteur, voient le management du risque sous des angles très différents. Dans les autres secteurs, les entreprises établies de longue date sont convaincues que leur propre façon d'aborder le risque répond amplement à leurs besoins[3].

Les réglementations Sarbanes-Oxley, Bâle II et III, la directive Solvabilité II, le cadre du COSO II (Committee of Sponsoring Organizations of the Treadway Commission) et la norme ISO 31000 sont les feuilles de route fondamentale du Risk management. En effet, dans la littérature, plusieurs définitions et approches de management du risque à noter. Nous avons à cet effet, sélectionné quelques unes d'entres elles qui nous paraissent êtres les plus significatives à notre recherche. Dont, nous illustrons dans le tableau suivant une grille des définitions proposée par Amadou Sienou.

Sienou dans le cadre de ses travaux sur le management intégré des risques et des processus, met l'accent sur quatre aspects caractérisant le management du risque ; soit en premier lieu, une analyse du « quoi » qui précisera sa nature, puis du « pourquoi » qui décrira sa finalité ainsi la structure qui définira les composantes d'organisation. En fin, le comportement qui désignera l'approche ou la discipline. Notant que l'entreprise constitue l'environnement des différentes définitions.

[1] Jérémie Lacroix; Analyse et gestion des risques dans les grandes entreprises: impacts et rôles pour la DSI; rapport réalisé dans le cadre du partenariat de recherche liant le CIGREF et l'IERSE; Paris; 2007; pp 14-15.
[2] Marc Fumey; op.cit; p56.
[3] Alice Underwood & David Ingram; L'étoffe de la GRE; La gestion du risque; Revue N°21; publié par la Society of Actuaries, Institut canadien des actuaires et Cosualty Actuarial Society; Mars 2011; p5.

Tableau N° 2 : Grille des définitions du Risk Management

Domaine	Auteur	Définition	Nature	Finalité	Structure	comportement
Management	IFRIMA, 1994	A management discipline whose goal is to ensure the survival of an organization by reducing the potential for loss before it occurs, and financing, through insurance and other means, potential exposures to catastrophic loss such as acts of God, human error or court judgments.	discipline de management	assurer la survie, réduction de pertes, financement d'expositions aux aléas	-	-
Management	IFRIMA, 1994	A systemic, statistically based, and holistic process that builds on a formal risk assessment and management, and addresses the set of four sources of failures within a hierarchical multi-objective framework of (i) hardware failure (ii) software failure (iii) organizational failure and (iv) human failure.	processus basé statistique	gérer les sources de défaillance	Apprécier gérer les risques	-
Sécurité industrielle	IFRIMA, 1994	A management function whose objective is the protection of people, assets and earnings by avoiding or minimizing the potential for loss from pure risks and the provision of funds to recover from losses that do occur.	fonction de management	protection des biens	Éviter, minimiser Les pertes, restaurer en cas de pertes	-
Management	IFRIMA, 1994	A management function that encompasses all activities directed towards attaining the optimum degree of avoidance, elimination or control of identified and assessed non-speculative human physical and financial risks throughout the Corporation	Ffonction de management	Optimiser le dégré de maitrise des risques	Identification, appréciation	-
Management	IFRIMA, 1994	The systematic application of management policies, procedures and practices to the tasks of identifying, analyzing, evaluating and controlling risk	Fonction de management	-	Identification, analyse, évaluation, maitrîse	Systélique
Management	DeLoach , 2000	A structured and disciplined approach: it aligns strategy, processes, technologies, and knowledge with the purpose of evaluation and managing the uncertainties the enterprise faces as it creates value	Démarche	Gestion des incertitudes	Alignement, évaluation, management	Structuré, discipliné
Management	Treasury Board of Canada, 2001	Une approche systémique servant à déterminer la meilleure voie à prendre en cas d'incertitude en identifiant, en évaluant, en comprenant, en communiquant les questions liées aux risques et en prenant des mesures à leur égard	Démarche	Améliorer les décisions sous incertitudes	Identifier, évaluer, comprendre, communiquer, traiter	Systématique
Ingéniere	NASA, 2002a	An organized, systematic decision making process that efficiently identifies, analyzed, plans, tracks, controls, communicates and documents risk to inrease the likelihood of achieving program / project goals	Processus de decision	Croitre la probabilité de succès	Identification, analyse, planning, suivi, communication, Documentation	systémique

Approche globale	ISO/IEC Guide73, 2002	Activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque	processus	Piloter l'organisme	-	Comportement
Management	AIRMIC et al, 2002	processus par lequel les organisations traitent méthodiquement les risques qui s'attachent à leurs activités et recherchent ainsi des bénéfices durables dans le cadre de ces activités, considérées individuellement ou bien dans leur ensemble	Processus	Recherche de bénéfices	-	Méthodique
Projet	ISO 17666, 2003	Systematic and iterative optimization of the project resources, performed according to the established project risk management policy	-	Optimisation des resources	-	Systématique, itérative
Assurance	Casualty Actuarial Society, 2003	the discipline by which an organization in any industry assesses, controls, exploits, finances, and monitors risks from all sources for the purpose of increasing the organization's short- and long-term value to its stakeholders	Discipline de management	Croitre la valeur de l'organisation	Apprécier, contrôler, exploiter, financer, suivre	-
Management	COSO, 2004	A process,…applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its appetite, to provide reasonable assurance regarding the achievement of entity objectives	Processus	Donner une confidence vis-à-vis de la réalisation des objectifs et positionner les risques dans l'intervalle de l'appétence	Identification, management	-
projet	PMI, 2004	the processes concerned with conducting risk management planning, identification, analysis, responses, and monitoring and control on a project	Processus	-	Planning, identification, analyse, réponse, suivi et contrôle	-
Publique	HM-Treasury, 2004	All the processes involved in identifying assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.	Ensemble de processus	-	Identifier, apprécier, responsabiliser, traiter, suivre, réviser	-
Management	AS/NZS 4360, 2004	The culture, processes and structures that are directed towards realizing potential opportunities whilst managing adverse effects	Culture, processus, organisation	Réaliser des opportunités tout en gérant les aléas négatifs	-	-
Sécurité SI	ISO/IEC JTC 1/SC 27, 2006	the process of identifying, controlling and eliminating or minimizing harmful events which may affect assets, at an acceptable cost	Processus	Protection des biens en optimisant les coûts	Identification, contrôle, maîtrise	-
Défense	DoD, 006	a continuous process that is accomplished throughout the life cycle of a system. It is an organized methodology for continuously identifying and measuring the unknowns; developing mitigation options; selecting, planning, and implementing appropriate risk mitigations; and tracking the implementation to ensure successful risk reduction	Processus, méthodologie	Assurer une réduction effective des risques	Identifier, mesurer, traiter, suivre	Itératif

Source : Amadou SIENOU; 2009 ; pp 65-66

Il est intéressant de souligner, dés à présent, que le management du risque d'entreprise est la traduction faite en France par le cabinet PriceWaterhouceCoopers et Landewell en association avec l'Institut français de l'audit et du contrôle interne ″IFACI″ de « Entreprise Risk Management – Integrated Framework, ERM » plus connu sous COSO II Report diffusé en 2004, qui est le prolongement de « Internal Control - Integrated Framework » connu sur COSO I Report, publié aux États-Unis en 1992[1].

Retournant au tableau ci-avant, il ressort que le management du risque d'un point de vue comportement et nature, est un processus ou discipline basée essentiellement sur une approche systémique, itératif qui se répète et évolue d'une manière continue. Concernant la structure, nous constatons que le management du risque est un ensemble d'activités de pilotage et de surveillance des aléas ou d'incertitude qui varient en fonction du domaine d'application.

Il est à noter que les composantes de la structure dans les différentes approches de management du risque sont quasi homogènes malgré la différence du vocabulaire ou des termes qui les désignent. D'une manière générale, on distingue à travers les objectifs, l'environnement et le planning du management du risque, un enchainement d'une phase opérationnelle, consistant en l'identification, l'analyse, l'évaluation, le traitement et le suivi des risques, ainsi une phase du reporting inclus une vision d'amélioration de la performance du processus.

Ces aspects présentent une certaine ambigüité, et par souci de clarté, nous compléterons cette revue de la littérature par la définition proposée sur le vocabulaire de « ISO 31000, 2009 », dont le management du risque est décrit étant qu'une approche de management qui relève de la culture de l'entreprise ou d'organisation d'un sens plus large, et se déploie par un processus « processus de management du risque ou cycle de management du risque »

En outre, Bénédicte Huot de Luze[2], la directrice scientifique de l'AMRAE, dans son article L'heure à l'efficacité de la gestion des risques, propose un ensemble des définitions. Dont, elle décrit le management du risque étant qu'une démarche itérative de diagnostic, de traitement et d'audit des risques de l'entité lui permettant d'atteindre ses objectifs avec un niveau d'aléa accepté.

Alors que, le management globale des risques, est la coordination des démarches de management du risque afin d'obtenir une vision sur l'ensemble des risques, leurs interaction et des priorités de l'entité. Ainsi, le système de management du risque est un ensemble composé de l'autorité, des ressources, des compétences et de l'organisation, permettant à une entité d'assurer le management globale de ses risques conformément à ses objectifs.

En fin, la finalité ou les objectifs du management du risque, présentent une grande diversité couvrant divers concepts comme le pilotage, la protection des biens, l'assurance raisonnable, l'amélioration et la création de la valeur, etc. À ce titre, nous aborderons cet aspect dans le point suivant.

2. Les finalités et les objectifs du Risk Management d'entreprise

Le comportement dynamique d'une entreprise est souvent lié aux notions de flexibilité et de réactivité; la flexibilité s'entend comme la capacité d'un système « d'une entreprise » à créer ou gérer la variété, de façon économique et continue, afin de s'adapter aux perturbations

[1] Eustache Ebondo Wa Mandzila et Daniel Zéghal; Management des risques de l'entreprise: Ne prenez pas le risque de ne pas le faire; La Revue des Sciences de Gestion; Direction et Gestion N° 237-238- Stratégie; Dossier: Innovations managériales; Mai-Août 2009; p18.

[2] Bénédicte Huot de Luze; L'heure à l'efficacité de la gestion des risques; la revue mensuel des Centraliens; Sep/Oct 2009; p5.

ou incertitude, externes ou internes, tout en maintenant son équilibre; tandis que la réactivité caractérise la capacité d'un système « d'une entreprise » de piloter à prendre en compte les perturbations et les aléas. La réactivité s'applique à tous les domaines : en conception afin de suivre, voire précéder le marché et intégrer les innovations technologiques; en production, afin de synchroniser les commandes et optimiser leur délai de réalisation grâce techniques d'ordonnancement; ainsi en logistique, pour synchroniser les approvisionnements aux lancements de production[1].

D'ailleurs, les entreprises se retrouvent aujourd'hui plus que jamais confrontées à la nécessité d'adapter des politiques du management du risque, permettant à anticiper et maîtriser les événements redoutés qu'ils soient susceptibles de subir. Aussi bien, in fine, le management du risque permet donc à l'entreprise d'assurer raisonnablement sa pérennité, image ainsi il consiste un facteur de sa compétitivité à long ou moyen terme.

- *La compétitivité*

Au contraire des systèmes de management tels que ceux développés pour gérer la qualité, les attentes à l'environnement ou la sécurité, qui s'appuient sur des normes (ISO 9001, 14000…) et considèrent que la réduction du risque est un but en soi, le management du risque est un système globale qui ne s'adresse pas à un risque particulier et qui surtout ne place pas la maîtrise du risque au centre du système mais vise l'optimisation économique de l'incertitude[2].

Le management du risque conduit l'entreprise à prendre des décisions basées sur une prise des risques calculées. Il va également permettre l'entreprise à estimer le coût potentiel d'un risque afin de déterminer le meilleur compromis entre les moyens financiers de prévention, protection et le coût d'identifications des risques; on verra ces concepts plus loin dans cette recherche.

Par conséquence, selon le cadre proposé par FERMA[3], le management du risque favorise l'amélioration de la qualité, de la réputation et l'optimisation des coûts; facteurs qui contribuent à la perception de la valeur de l'entreprise. Dont, le management du risque s'établit comme une démarche pour assurer la protection des biens, prévenir des crises en limitant les pertes spontanées et assurer la pérennité des avantages concurrentiels et donc la compétitivité de l'entreprise.

- *La pérennité*

Suite à la lecture du tableau N°2, le management du risque contribue à la création et la préservation de la valeur d'entreprise, par l'amélioration de processus de décision et de planification vis-à-vis des alternatives confrontant l'activité de l'entreprise. En effet, il permet de choisir un ensemble d'options de traitement en adéquation avec l'impact du risque et de l'appétence pour le risque; il contribue également, à l'optimisation de l'utilisation et l'allocation du capital et des ressources d'entreprise[4].

En outre, le management du risque établit un lien entre la croissance d'entreprise et le niveau d'exposition au risque, dont, il ajuste les attentes d'entreprise en relation avec les objectifs de gain et les risques.

[1] Elena Loredana Podea; op.cit; p46.
[2] Bernard Barthélemy et Philippe Courréger; La gestion des risques : Méthode d'optimisation globale; 2ème Éditions d'Organisation; Paris; 2004.p 34.
[3] Federation of European Risk Management Associations; Cadre de référence de la gestion des risques; FERMA; Belgium; 2003. www.firma.eu
[4] Federation of European Risk Management Associations; op.cit; p5.

- *L'image*[1]

Une bonne communication autour du processus et programme de management du risque vis-à-vis les parties prenantes, peut être un facteur d'amélioration de l'image de marque de l'entreprise; par exemple, en interne, en témoignant de l'engagement de la direction en matière de sécurité et donc de protection du personnel et de sécurisation de l'emploi.

Le management de risques d'entreprise adopte une vision de la responsabilité sociétale, par la protection et la préservation des ressources naturelles et l'hygiène industrielle. Ainsi, le management du risque soutient le développement durable (Sustainability, Social accountability).

Il est toute fais important de noter que les objectifs de management du risque se déférent en fonction du domaine d'activité d'entreprise. Dans ce cadre The Economist Intelligence Unit a réalisé une étude portée sur la pondération de chaque objectif par rapport au secteur d'activité d'entreprise, comme suite :

Tableau N°3 : Les différents objectifs de management du risque d'entreprise en fonction du secteur d'activité

Le secteur économique / Les objectifs de l'analyse et de la gestion du risque	Les services financiers	Commerce en détail/Produits de large consomme	Industrie	Télécommunications High-Tech	Utilisation/Ressources naturelles	Chimie/Industrie pharmaceutique
Identification des facteurs de risque où l'entreprise est exposée	67%	58%	71%	64%	70%	67%
Obtention d'un avantage compétitif par une bonne connaissance de facteurs de risques	73%	54%	67%	43%	75%	73%
Protection devant les pertes	67%	54%	46%	71%	65%	73%
Faire face aux risques externes	56%	50%	38%	79%	45%	67%
L'optimisation de l'allocation des ressources internes	58%	46%	63%	29%	35%	60%
Allocation efficiente du capital	65%	35%	54%	43%	65%	40%
Evitation des risques	60%	39%	21%	71%	55%	47%
Identification des risques avec l'effet radical	46%	50%	38%	21%	40%	40%
Flexibilité organisationnelle	44%	39%	29%	43%	40%	53%
Amélioration PER (price earning ratio)	44%	35%	42%	43%	25%	33%
Réduction des coûts pour couvrir les risques (assurence etc.)	33%	42%	38%	57%	20%	53%

Source: Business Finance Magazine, 2002, http:// business financemag.com.

Nous retiendrons également les objectifs de management du risque cités sur le cadre du COSO2; ce cadre référentiel vise à aider l'entreprise à atteindre ces objectifs qu'on peut les classer dans les quatre catégories suivantes[2]:

- *Stratégique*: objectifs stratégiques servant la mission de l'entreprise.
- *Opérationnel* : objectifs visant l'utilisation efficace et efficiente des ressources.

[1] Bernard Barthélemy et Philippe Courréger; op.cit; p36.
[2]The Committee of Sponsoring Organizations of the Treadway Commission (COSO); Enterprise Risk Management - Integrated Framework: Executive summary; September 2004; p3.

- *Reporting* : objectifs liés à la fiabilité du reporting.
- *Conformité* : objectifs de conformité aux lois et aux réglementations en vigueur.

Certes, que le rattachement de ces objectifs à différentes catégories permet de se concentrer sur les différents aspects de management du risque, nous reviendrons sur ces points un peu plus loin. Tous en étant distinctes, ces catégories se recoupent, un objectif donné peut relever de plusieurs d'entre elles, et répondent aux divers besoins de l'entreprise. Notant que le management du risque ne peut offrir qu'une assurance raisonnable quant à la réalisation de ces objectifs et la maîtrise des opérations. Comme tout système, il peut avoir des limites, cela peut aller d'une défaillance humaine à de mauvais jugements exercés lors de la prise de décision, ou même d'une simple erreur commise lors du déroulement du processus.

En termes simples, indique André Choquet, président de la Commission des applications en management du risque d'entreprise de l'Institut canadien des actuaires, « ERM consiste à recueillir de l'information et à la structurer, de façon à pouvoir prendre des décisions éclairées qui permettront d'accroître la valeur à long terme de l'entreprise. Auparavant, le management du risque, consistait, dans bien des cas, à respecter la réglementation, plutôt qu'un cadre chargé de la conformité qui comprend bien les grands risques stratégiques découlant des diverses unités organisationnelles et facilite la prise de décisions claires, depuis le conseil d'administration jusqu'aux divers secteurs d'activités [1]».

3. Entreprise Risk Management : le cadre normatif et référentiel

Le risk management ou le management du risque est une discipline qui a été, pour longtemps, peu formalisée. Des théories organisationnelles et économiques s'élaborent autour de concepts, de méthodes et d'outils nouveaux; des cabinets de consulting proposent leurs expertise alors que plusieurs cadres législatifs désormais la notion de management du risque. En outre, les approches sont souvent spécifiques à une entreprise, à son activité, à sa culture, à son type d'organisation.

En fin, le risk management est l'objet de nombreux standards et bien qu'ils n'aient pas souvent de portée obligatoire, ils permettent en général d'obtenir un avantage compétitif malgré que la certification dans ce domaine reste assez floue, où elle est rattachée aux référentiels de la qualité, désormais de multiples organismes officiels du Risk Management « AMRAE en France, IRM au Royaume-Uni et FERMA en Europe [*]», ayant donné naissance à divers cadre de référence[2].

En 2006, FERMA en collaboration avec AXA Corporate Solutions et Ernest & Young ont d'ailleurs effectué une enquête sur les pratiques du ERM[*], auprès de 460 entreprises dans différents secteurs d'activités pour 16 pays européens. Cette enquête montre que les cadres de référence de management du risque « COSO II et FERMA/AIRMIC » sont maintenant bien connus, par, respectivement 70% et 61% des entreprises européens[3].

---

[1]Institut canadien des actuaires; La gestion du risque d'entreprise: devriez-vous instaurer la gestion du risque d'entreprise? ; Actuaires. CA; 2007; p2.

[*]Voir annexe N°1.

[2]David Autissier, Faouzi Bensebaa et Fabienne Boudier; L'Atlas du management; Éditions d'organisation Eyrolles; Paris; 2009; p217.

[*] FERMA en collaboration avec AXA CS et Ernest & Young réalisent tous les deux ans depuis 2002, une édition sur le pratique de management du risques en Europe.

[3] Jean-Claude Tourneur; les pratiques de gestion des risques; Dossier: les processus de maîtrise des risques évoluent; Le magazine de la normalisation et du management; AFNOR; N°278; Octobre 2007; p 37.

Dans le même contexte, la 5éme édition de l'étude FERMA figure que ces référentiels COSOII et FERMA/AIRMIC sont adaptés par, respectivement 30%, 23% parmi 782 entreprises européens; tandis que la norme ISO 31000 demeure à ce stade une référence mineure par 13%. Et encore 47% des entreprises ne font toujours référence à aucun standard dans leur pratique de management du risque[1].

À ce point, nous proposons dans d'en définir de quoi s'agit une norme ou une référence, pour en suite décrire un aperçu sur la conception et la structure de la plus récente norme de management du risque (ISO/IEC 31000:2009) étudié jusqu'ici. Et enfin, établir une comparaison des quatre principaux référentiels de management du risque d'entreprise.

Les normes et les référentiels : définitions

Les entreprises, les administrations nationales ou internationales, les organisations s'appuient sur des normes, des référentiels, des méthodes et des modèles, dans l'objectif de rester compétitives. La maîtrise de ces outils représente un atout important, voire stratégique, pour toutes. Par exemple, la qualité, le coût, le délai et le respect de l'environnement sont des critères importants et incontournables pour l'ensemble des acteurs qui appartiennent à la chaîne logistique normale.

Commençant par la définition de la norme[2], officiellement l'ISO et IEC la définie comme un « Document établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats garantissant un niveau d'ordre optimal dans un contexte donné ».

En effet, la norme est élaborée, définie, officialisée et publiée par un organisme de normalisation. Elle a pour but de définir un standard, des directives, des règles à suivre afin de concevoir, produire un service, un produit, un bien qui soit conforme aux attentes du marché. Elle doit prendre en compte les aspects qui sont liés à la sécurité et à l'environnement.

La norme est proche de la directive réglementaire; à ce titre elle doit être suivie par les entreprises qui sont concernées par son utilisation, et cela quel que soit le pays ou le type d'entreprise.

La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, les biens et les services qui se posent de façon répétée dans des relations entre partenaires économiques, techniques, scientifiques et sociaux.

Parmi les principaux organismes de normalisation internationaux, on cite l'ISO, CEI; comme on trouve des organismes nationaux tels que AFNOR, JSA, AMRAE …etc. (voir annexe N°1)

Revenant sur la définition d'un référentiel de certification[3], qui est un ensemble de recommandations qui composent un produit industriel, ou un processus, ou un service. Un référentiel est élaboré au préalable par une organisation réunissant un ensemble d'experts.

Un référentiel peut s'aider d'une norme, ou devenir une norme. Nous avons l'exemple du référentiel ITIL qui s'est décliné en la norme ISO 20000*.

[1] Dominique Pageaud (Ernst & Young) et Régis Demoulin (AXA CS); Tendances et pratiques de la gestion des risques en Europe-étude comparative; FERMA; 2010; p6.
[2] Gilles Teneau, Jean-Guy Ahanda; Guide commenté des normes et référentiels; Éditions d'Organisation; Groupe Eyrolles; Paris; 2009; p 17 et 19.
[3] Idem; p 102-103.
* Norme pour les organisations qui fournissent des services, processus d'audit.

Les référentiels de certification peuvent être de deux types :

- Les référentiels de certification des hommes, tel ITIL (Information Technology Infrastructure Library).
- Les référentiels de certification des organisations, tel EFQM (European Foundation for Quality Management).

Un référentiel de certification comporte :

✓ Les méthodes de mesure, d'analyse, de test ou d'évaluation.
✓ Les engagements pris par les prestataires.
✓ La nature et le mode de présentation des informations considérées comme essentielles.
✓ Les caractéristiques retenues pour décrire les produits ou les services.
✓ Les modalités des contrôles auxquels procède l'organisme certificateur.
✓ Les rôles et les responsabilités attribués aux personnes en charge du référentiel.
✓ Un ensemble de processus, organisés en structure, en stratégie et en gestion des hommes.

3.1. Le référentiel COSO et l'Enterprise Risk Management

C'est dans la perspective de permettre aux dirigeants de disposer de systèmes plus efficaces, efficients et éthiques dans les affaires quotidiennes, que le comité COSO « Committee Of Sponsoring Organizations of the Treadway commission » a été créée en 1985, organisation bénévole du secteur privé, réunissant les compétences d'un certain nombre de professionnels, de quelques cabinets d'audit externe et de grandes entreprises américaines; ce comité présidé par « Larry E-Rittenberg », est l'émanation de cinq associations professionnelles:

- American Accounting Association, AAA ;
- American Institute of Certified Public Accountants, AICPA ;
- Financial Executive International, FEI ;
- Institute of Management Accountants, IMA ;
- The Institute of Internal Auditors, IIA* .

Le succès du COSO en tant que cadre de référence du contrôle interne est dû à son utilisation comme outil de mise en œuvre des lois de sécurité financière, notamment aux États-Unis (Sarbanes Oxley Act-SOX) et en France (Loi de Sécurité Financière-LSF). Aussi, qu'il est sponsorisé et divulgué au niveau mondial un cadre conceptuel et des directives basées sur des analyses, des recherches approfondies et des meilleures pratiques[1].

COSO-I « Internal Control–Integrated Framework »

En 1992, Ce comité a édité son premier ouvrage, un rapport sur le cadre référentiel de contrôle interne appelé COSO-I « Internal Control–Integrated Framework », traduit en français sous le titre « La pratique du contrôle interne ». Le COSO-I définit un modèle conceptuel dont chaque entreprise peut s'inspirer comme référentiel pour renforcer et améliorer les systèmes de contrôle, ce référentiel a évolué depuis 2002 vers un second corpus dénommé COSO-II « Enterprise Risk Management-Integrated Framework » publié en 2004.

* l'IIA « Institute of Internal Auditors – www.theiia.ogr , traduit en français par l'IFACI « Institut Français de l'Audit et du Contrôle Interne – www.ifaci.com

[1] Philippe Norigeon; Système d'information et contrôle interne de l'entreprise dans un contexte d'expertise judiciaire; Commission Economie et Finance; le 17/12/2009; p 10.

En effet, le COSO-I définit le contrôle interne, décrit ses composantes et fournit des critères par lesquels les systèmes de contrôle peuvent être évalués; le contrôle interne y est défini étant un processus mis en œuvre par le conseil d'administration, les dirigeants et le personnel d'une organisation, destiné à fournir une assurance raisonnable quant à la réalisation des trois objectifs suivants[1] :

- L'efficacité et l'efficience des opérations ;
- La fiabilité des informations financières :
- La conformité aux lois et règlements.

En effet, le référentiel COSO-I a donné naissance à une pyramide et un cube dont ses trios faces visibles présentent trois objectifs et cinq composantes essentiels jugés nécessaires pour une bonne maîtrise des activités d'entreprise ; ces éléments illustrés sur la figure ci-après, présentent les conditions indispensables pour un bon contrôle interne.

Figure N°6 : La pyramide et le cube du COSO-I« Internal Control–Integrated Framework »

Source : Walter Hunziker ; 2009 ; p18[2].

Il ressort que la pyramide du COSO-I montre l'interaction entre les composantes du contrôle interne, tandis que le cube reflète le rapport entre ces composantes et les entités ou les activités ainsi les objectifs de l'entreprise.

Ce référentiel indique que le contrôle interne est constitue de cinq composantes misent en synergie, qui découlent de façon dont la direction exploite sont entreprise et qui sont intégrées au processus de management [3]:

- L'environnement de contrôle interne ;
- L'évaluation des risques ;

[1] COSO; Internal Control- Integrated Framework: Guidance on Monitoring Internal Control Systems; COSO Publication; September 2007; p3.
[2] Walter Hunziker : Chef du contrôle cantonal des finances du canton de zoug & Expert-réviseur agrée ASR; Système du contrôle interne avec COSO; Economiste d'entreprise HES/CIA; le 08/09/2009; p18.
[3] Bernard GUMB et Christine NOËL; Le rapport des dirigeants sur le contrôle interne à l'épreuve de l'analyse de discours; Revue de Comptabilité Contrôle Audit; Tome 13; N°2; Décembre 2007; p102.

- Les activités de contrôle interne ;
- L'information et la communication ;
- Le pilotage.

Chacune de ces composantes est déclinée sur chaque activité et fonction de l'entreprise.

Reprenons brièvement ces cinq composantes du contrôle interne sous le COSO-I[1] :

✓ **L'environnement de contrôle interne** : Il constitue le fondement de tous les autres éléments du contrôle interne; incluant l'intégrité, les valeurs éthiques, le modèle de fonctionnement du management, la délégation des systèmes de direction, et aussi les procédures de développement du personnels de l'entreprise ;

✓ **L'évaluation des risques** : L'entreprise doit être consciente des risques et les maîtriser. Elle doit fixer des objectifs et les intégrer aux activités, afin de fonctionner de façon harmonieuse. Elle doit également instaurer des mécanismes permettant d'identifier, analyser et gérer les risques correspondants ;

✓ **Les activités de contrôle interne** : Les normes et procédures de contrôle doivent être élaborées et appliquées pour s'assurer que sont exécutées efficacement les mesures identifiées par le management comme nécessaires à la maîtrise des risques liés à la réalisation des objectifs ;

✓ **L'information et la communication** : Les systèmes d'information et de communication sont articulés autour de ces activités de contrôle. Ils permettent au personnel de recueillir et échanger les informations nécessaires à la conduite et au contrôle des opérations ;

✓ **Le pilotage** : L'ensemble du processus doit faire l'objet d'un suivi et des modifications doivent y être apportées le cas échéant. Ainsi, le système peut réagir rapidement en fonction du contexte.

Ces composantes, en constante interaction constituent toute la dynamique du contrôle interne. Dans l'environnement de contrôle, les dirigeants évaluent les risques susceptibles d'altérer les activités et freiner la réalisation des objectifs d'entreprise; dont, des mécanismes sont mis en place afin de s'assurer de l'efficacité des mesures prises en vue de maîtriser les risques encourus. De manière continue, les informations pertinentes sont recueillies et communiquées à l'ensemble de l'organisation. Ce processus de contrôle interne est régulièrement piloté afin de déceler d'éventuels dysfonctionnements et apporter les modifications nécessaires.

Nous approfondirons dans la section suivante ces éléments du contrôle interne ainsi sa contribution dans la maîtrise et la surveillance des risques d'entreprise.

COSO-II « Enterprise Risk Management–Integrated Framework »

Au tout début des années 2000, le COSO a demandé à PricewaterhouseCoopers, déjà coauteur du COSO-I de développer un référentiel méthodologique pour le management du risque intégré dans l'ensemble des composantes de l'entreprise. Ce référentiel a été publié en septembre 2004 sous le titre « Enterprise Risk Management-Integrated Framework ». Dont la version française a été publiée en 2005 par PricewaterhouseCoopers (PwC) et Landwell en association avec l'Institut Français de l'Audit et du Contrôle Interne (IFACI)[2]. Ce référentiel

[1] AMF; Le dispositif de Contrôle Interne : Cadre de référence; Publication de l'autorité des Marchés Financiers; Janvier 2007; p5.
[2] Xavier Maitrier*; Le management par les risques : enjeux et perspectives; Les Echos : L'Art du Management; Stratégie et gouvernance; N°9/10; Jeudi 8 décembre 2005; p4.

appelé aussi COSO-II s'inscrit dans le prolongement du COSO-I, il apporte une approche tournée plus vers le management du risque dans un environnement soumis à l'incertitude.

Le référentiel COSO-II établi à la suite du Sarbanes-Oxley Act aux États-Unis ne remplace pas le cadre de COSO I, mais le complète et le renforce en ajoutant au classement par nature « opérations, reporting et conformité » une dimension stratégique et en précisant le découpage par destination « niveau entreprise, direction, unités opérationnelles et niveau filiales ».

En fait, comme le rapport COSO-I est un référentiel du contrôle interne, le COSO-II est plutôt un référentiel de management du risque. Selon le COSO, le management du risque est affirmé comme le préalable nécessaire à un contrôle interne efficace et satisfaisant, d'où l'on déduit parfois que le contrôle interne est inclus dans le management du risque.

Comme nous l'avons déjà mentionné, Le COSO-II donne le management du risque d'entreprise la définition suivante :

« *Le management du risque est un processus mis en œuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs*. *Il est pris en compte dans l'élaboration de la stratégie de l'entreprise ainsi que dans toutes les activités et conçu pour identifier les événements potentiels pouvant affecter l'entreprise et gérer les risques dans les limites de son appétence pour le risque afin de donner une assurance raisonnable quant à la réalisation des objectifs de l'entreprise* »

Ce référentiel COSO-II, précise que la valeur de l'entreprise est maximisée d'une part lorsque la direction élabore une stratégie et fixe des objectifs afin de parvenir à un équilibre optimal entre les objectifs de croissance et de rendement et les risques associés, et d'autre part lorsqu'elle déploie les ressources adaptées permettant d'atteindre ces objectifs.

Le dispositif de management du risque comprend les éléments suivants [1]:

- **Aligner l'appétence pour le risque avec la stratégie de l'entreprise** : L'appétence pour le risque est une donnée que la direction prend en considération lorsqu'elle évalue les différentes options stratégiques, détermine les objectifs associés et développe le dispositif pour gérer les risques correspondants ;
- **Développer les modalités de traitement des risques** : Le dispositif de management du risque apporte une méthode permettant de choisir de façon rigoureuse parmi les différentes options de traitement des risques « l'évitement, la réduction, le partage ou l'acceptation du risque » ;
- **Diminuer les déconvenues et les pertes opérationnelles** : L'entreprise améliore sa capacité à identifier et traiter les événements potentiels, ce qui permet d'atténuer les impondérables et de diminuer les coûts ou pertes associés ;
- **Identifier et gérer les risques multiples et transverses** : Chaque entité est confrontée à une multitude de risques affectant différents niveaux de l'entreprise. Le dispositif de management du risque renforce l'efficacité du traitement des impacts en cascade et apporte des solutions intégrées pour les risques à conséquences multiples ;

*Xavier Maitrier : est associé de PricewaterhouseCoopers, responsable du département amélioration de la performance, risques et contrôle interne de PwC en France. Il anime le comité pluridisciplinaire risques et contrôle interne de PwC et Landwell & Associés, cabinet d'avocats correspondant de PwC.

[1] Philippe Christelle (Président de IFACI) et Serge Villepelet (Président de PwC); Le management des risques d'entreprise : Cadre de référence - Techniques d'application du COSO II Report; Synthèse de l'ouvrage; IFACI, PwC et Landwell; Éditions d'Organisation; France; 2005; pp 3-4.

- **Saisir les opportunités** : C'est en prenant en compte un large éventail d'événements potentiels que la direction est le mieux à même d'identifier et de tirer parti des opportunités de façon proactive.
- **Améliorer l'utilisation du capital** : C'est en ayant une vision claire des risques de l'entreprise que la direction peut évaluer efficacement les besoins en capitaux et en améliorer l'allocation.

Ces éléments du dispositif de management du risque contribuent à la réalisation des objectifs de performance et de rentabilité d'entreprise. Dont, le dispositif de management du risque contribue à la mise en place d'un reporting efficace et au respect de la conformité aux lois et réglementations ; aussi bien, il protège l'image et la réputation de l'entreprise

Comme le montre la figure N°7, la novation fondamentale du COSO-II est dans l'exigence d'une approche globale de l'appréciation du risque, une approche résumée en quatre objectifs, huit composantes, des conditions indispensables l'efficacité du management du risque :

- **Face supérieure du cube : Les objectifs de l'entreprise**

Selon COSO-II, les objectifs sont classés en quatre catégories :

- Objectifs stratégiques : objectifs de niveau le plus élevé, liés à la stratégie et de la mission de l'entreprise ;

- Objectifs opérationnels : objectifs généraux visant l'utilisation efficace et efficiente des ressources ;

- Objectifs de reporting : axés sur la fiabilité des informations financière et non-financiarises externe et interne pour le reporting ;

- Objectifs de conformité : relatifs à la conformité aux lois et règlements en vigueur.

- **Face avant du cube : Les composantes de management du risque**

En outre, le référentiel COSO-II décrit le dispositif de management du risque en huit composantes intégrées au processus de management :

- Environnement interne favorable « Internal Environment » : C'est la substitution de l'environnement de contrôle interne dans le COSO-I. il constitue le fondement structurel du système de management du risque et qui intègre des aspects très divers tels que la culture du risque, l'appétence pour le risque, l'intégrité et les valeurs éthiques, l'engagement de compétence, la structure organisationnelle, les délégations de pouvoirs et de responsabilités, la politique et l'environnement dans lequel l'entreprise opère ;

- Fixation des objectifs « Objectives Setting » : Les objectifs doivent avoir été préalablement définis pour que le management puisse identifier les événements potentiels susceptibles d'en affecter la réalisation. Le management du risque permet de s'assurer que la direction a mis en place un processus de fixation des objectifs et que ces objectifs sont en ligne avec la mission de l'entité ainsi qu'avec son appétence pour le risque ;

- Identification des événements « Ivent Identification »: Les événements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une entreprise doivent être identifiés en faisant la distinction entre risques et opportunités. Les opportunités sont prises en compte lors de l'élaboration de la stratégie ou au cours du processus de fixation des objectifs ;

- Évaluation des risques « Risk Assessment » : Les risques sont analysés, tant en fonction de leur probabilité d'occurrence que de leur impact, cette analyse servant de base pour déterminer la façon dont ils doivent être gérés. Les risques inhérents et les risques résiduels sont évalués ;

- Traitement des risques « Risk Response » : C'est-à-dire la décision qui doit être prise suite à l'évaluation des risques. Parmi les solutions et les alternatives possibles permettant de faire face aux risques, on choisira entre l'évitement (supprimer le risque en cessant l'activité à l'origine du risque), la réduction (mettre en œuvre des dispositions pour réduire la probabilité et/ou l'impact du risque), le partage (recours à l'assurance, à des opérations de couvertures ou l'externalisation de l'activité concernée), ou enfin l'acceptation (compte tenu accepter le risque en l'état). Pour ce faire le risk manager élabore un ensemble de mesures permettant de mettre en adéquation le niveau des risques avec le seuil de tolérance et l'appétence pour le risque de l'entreprise ;

- Activités de contrôle « Control Activities » : Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et à l'application effective des mesures de traitement des risques.

Ces dispositions regroupent des modalités telles que : les revues du management, la supervision directe d'une activité ou d'une fonction, la séparation des taches, les contrôles intégrés dans le traitement de l'information, les contrôles physiques, les indicateurs de performance ;

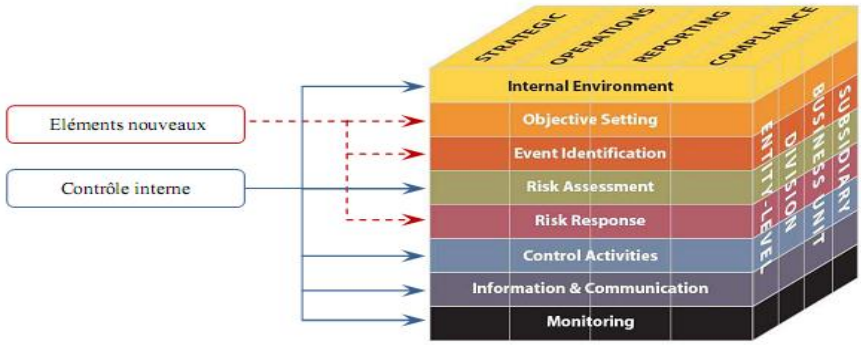
- L'information et la communication : Les informations pertinentes sont identifiées, collectées, saisies et communiquées ans un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'entreprise de façon efficace ;

- Le pilotage « Monitoring » : Il s'agit bien des activités quotidiennes de contrôle par le management que des démarches d'auto-évaluation ou encore de l'intervention des auditeurs internes ou externes.

- **La face latérale du cube : Filiale, Unité, Division et l'Entreprise**

Cette face symbolise le caractère multidimensionnel de management du risque et la nécessité de l'adapter au niveau d'entité concerné. En fait, nombreux paramètres peuvent impacter le management du risque tels que la taille de l'entreprise, sa culture du contrôle, son secteur d'activité, les réglementations en vigueur…etc.

Figure N°7 : Le cube du COSO-II « ERM–Integrated Framework »



Source: The Institute of Internal Auditors IIA; 2004[1].

Comme il apparaît par la description des deux rapports du COSO, le référentiels du management du risque COSO-II enrichi et complète le COSO-I sur quatre axes.

Reprenons l'axe des objectifs, comme nous avons déjà cité, sur le quel le COSO-II apporte un quatrième élément lié aux objectifs stratégiques.

Encore, sur l'axe de ***reporting*** est plus large sur COSO-II, il couvre désormais non seulement le reporting financier, mais aussi d'informations non-financières. De plus, il touche à la fois la communication interne et externe.

L'axe ***organisation*** est plus détaillé sur le COSO-II, avec une décomposition par niveaux portant impérativement sur toute l'entreprise, afin de pouvoir être croisée avec la stratégie.

Enfin, l'enrichissement de l'axe des composantes de ***contrôle interne*** du COSO-I, qui devient celui des composantes de management du risque. Le nombre des composantes passe de cinq à huit :

- L'élément « environnement » n'est plus seulement de contrôle. Il devient environnement interne et porte la notion d'appétence au risque « risk appetit » qui doit être pris en compte dans la définition de la stratégie de l'entreprise.
- L'élément « évaluation des risques » se décompose en quatre sous-éléments : la fixation des objectifs, l'identification des évènements, l'évaluation des risques et le traitement des risques.
- Les trois autres éléments (activités de contrôle, information et communication, pilotage) restent pratiquement inchangés par rapport au COSO-I.

De même, le COSO-II souligne l'importance de la prise de responsabilité de management du risque dans l'entreprise par la direction générale, le conseil d'administration, le Risk manager, le directeur financier, l'audit interne le contrôle interne et d'autres intervenants et collaborateurs de l'organisation d'entreprise.

3.2. La nouvelle norme d'ERM : Aperçu sur les lignes directrices de l'ISO 31000

« Risk Management - Principles and guidelines » traduit en français par « Management du risque - Principes et lignes directrices », voilà le titre de la nouvelle norme internationale sur le management du risque; aussi désignée la norme ISO 31000, elle est publiée en novembre 2009 et a été élaborée par un groupe de travail composé notamment de conseillers techniques de plus de 20 pays. Le groupe, qui s'est réuni à six reprises au cours de plusieurs années, a passé en revue la norme de management du risque en vigueur en Australie/Nouvelle-Zélande

[1] IIA; Applying Enterprise Risk Management-Integrated Framework, Presentation produced by The Institute of Internal Auditors IIA; September 29, 2004 ; www.coso.org .

« AS/NZS 4360:2004 - Risk management » dans le but de mettre au point une norme pouvant être appliquée par toute une gamme d'organisations dans n'importe quel pays et pour n'importe quel type d'activité, peu importe la complexité, la taille ou le genre.

La nouvelle norme fait renvoi à des définitions qui figurent dans un document connexe de l'ISO, le Guide « ISO/IEC73 - Risk management - Vocabulary », également publié en novembre 2009, qui représente une compilation de définitions et de termes en rapport avec le risque. La norme sur les techniques d'évaluation des risques ISO 31010, également diffusée en novembre 2009, est un autre document connexe[1]. De même cette norme ISO 31000 fut publiée avant d'être rapidement adoptée en norme française par AFNOR sous NF ISO 31000 en janvier 2010[2].

Tout a commencé lorsque le comité technique mixte Standards Australia/Standards New Zealand a élaboré la norme AS/NZS 4360 – Risk Management, qui a été publiée en novembre 1995, puis révisée en 1999 et plus récemment en 2004. Les organismes de normalisation du Canada (1997) et du Japon (2001) ont suivi avec leurs propres versions, puis en 2002, l'ISO et la Commission électrotechnique internationale (IEC) ont publié le Guide ISO/IEC 73:2002.

La norme AS/NZS 4360 répondait au besoin global d'un guide générique pour l'application d'un processus de management du risque dans les organismes et entreprises de tous types, tant privés que publics.

Faisant suite à la publication du guide ISO/IEC 73:2002, une proposition a été présentée au Bureau de gestion technique (TMB) de l'ISO en 2004, identifiant le besoin d'une norme ISO sur le management du risque.

Après avoir examiné la proposition lors de plusieurs réunions, le TMB a invité en septembre 2004, le Comité japonais des normes industrielles (JISC) à soumettre une proposition d'étude nouvelle (NWIP) pour la création d'un Groupe de travail (GT) chargé d'élaborer la norme.

A sa réunion de février 2005, le TMB a approuvé la distribution à tous les comités membres de l'ISO de la NWIP sur le management du risque soumise par le JISC (Japon).

À sa réunion en juin 2005, le TMB a confirmé la création d'un groupe de travail, GT, chargé de traiter de management du risque, qui est présidé par M. Kevin Knight de l'Australie et dont le secrétariat est assuré par le Japon. La réunion inaugurale a eu lieu à Tokyo en septembre 2005, les réunions suivantes à Sydney et Vienne en 2006 et à Ottawa en avril 2007[3].

En juin 2007, la rédaction du premier document de comité ISO/CD 31000 (Commitee Draft), et en avril 2008, le lancement de l'enquête et la rédaction de projet de norme internationale ISO/DIS 31000:2008 (Draft International Standard)[4].

Le 15 novembre 2009, la publication de la première édition de la norme Risk Management ISO 31000, pour ensuite être diffusée par AFNOR sous NF ISO 31000 en janvier 2010.

[1] Dorothy Gjerdrum & Mary Peter; La nouvelle norme internationale sur la pratique de la gestion du risque - Une comparaison entre la norme ISO 31000:2009 et le cadre GRE du COSO; La gestion du risque; Revue N°21; publié par la Society of Actuaries, Institut canadien des actuaires et Cosualty Actuarial Society; Mars 2011; p9.

[2] Bulletin de veille du CRDD; Centre de ressources documentaires du développement durable; Ministère de l'Écologie du Développement durable, des Transports et du Logement; N°04; Avril 2011; p21. www.crdd.developpement-durable.gouv.fr

[3] Kevin W. Knight; La future norme ISO 31000 sur le management du risque; Publication ISO Management Systems; Juillet-Août 2007; p10-11. www.iso.org/ims

[4] Stéphane Mathieu; ISO 31000 : Management du risque; Atelier d'échanges; Saint-Denis; Afnor Groupe; France; le 5 juin 2008; p6-7.

Comme l'indique son titre, la norme ISO 31000 établit des lignes directrices, elle n'est pas destinée pour des besoins de certification, mais soit un document de recommandations.

François Boucher, le chef de projet NF ISO 31000 chez AFNOR, indique que « its aim is to harmonize the risk management process and the definitions attached to it in existing and future standards, to encourage a risk culture and offer recommendations on implementing a risk management process…, it will be the reference framework for dealing with this issue. In this way, everyone will be speaking the same language…, ISO 31000 therefore introduces a methodology to help identify and manager any event that may have an influence, positive or negative, on the achievement of a target…, as well as being an organizational and operational framework, ISO 31000 also aims to make it easier to link up with other management system standards[1]».

En effet, cette norme a été élaborée pour aider les entreprises à intégrer les incertitudes de tout ordre dans leur système de management global, elle a pour ambition d'harmoniser le processus de management du risque avec les normes existantes, telles que dans les domaines de la qualité (ISO 9001), de l'environnement (ISO 14001), de la santé et la sécurité au travail (OHSAS 18001), ou de la responsabilité sociétale (SA 8000) ; aussi, des systèmes d'information (ISO 27000) ou de chaîne logistique (ISO 28000).

L'ISO 31000 définit un certain nombre de principes visant à rendre le management du risque plus efficace. Elle recommande aux entreprises d'élaborer, appliquer et améliorer continuellement un cadre pour intégrer le processus de management du risque dans la gouvernance, la stratégie et planification, le management, le processus de reporting, ainsi que de la politique, les valeurs et la culture.

Cette norme peut être utilisée par tous organismes, entreprise privée ou publique, association, groupe ou individu; elle peut être appliquée à une large gamme d'activité incluant la stratégie et les prises de décisions, les opérations, les processus, les fonctions, les projets, les produits et les services, etc. Elle propose un référence unique adaptable et suffisamment flexible pour qu'il s'applique à tous les types des risques faisant peser une incertitude sur l'atteinte des objectifs de l'organisme.

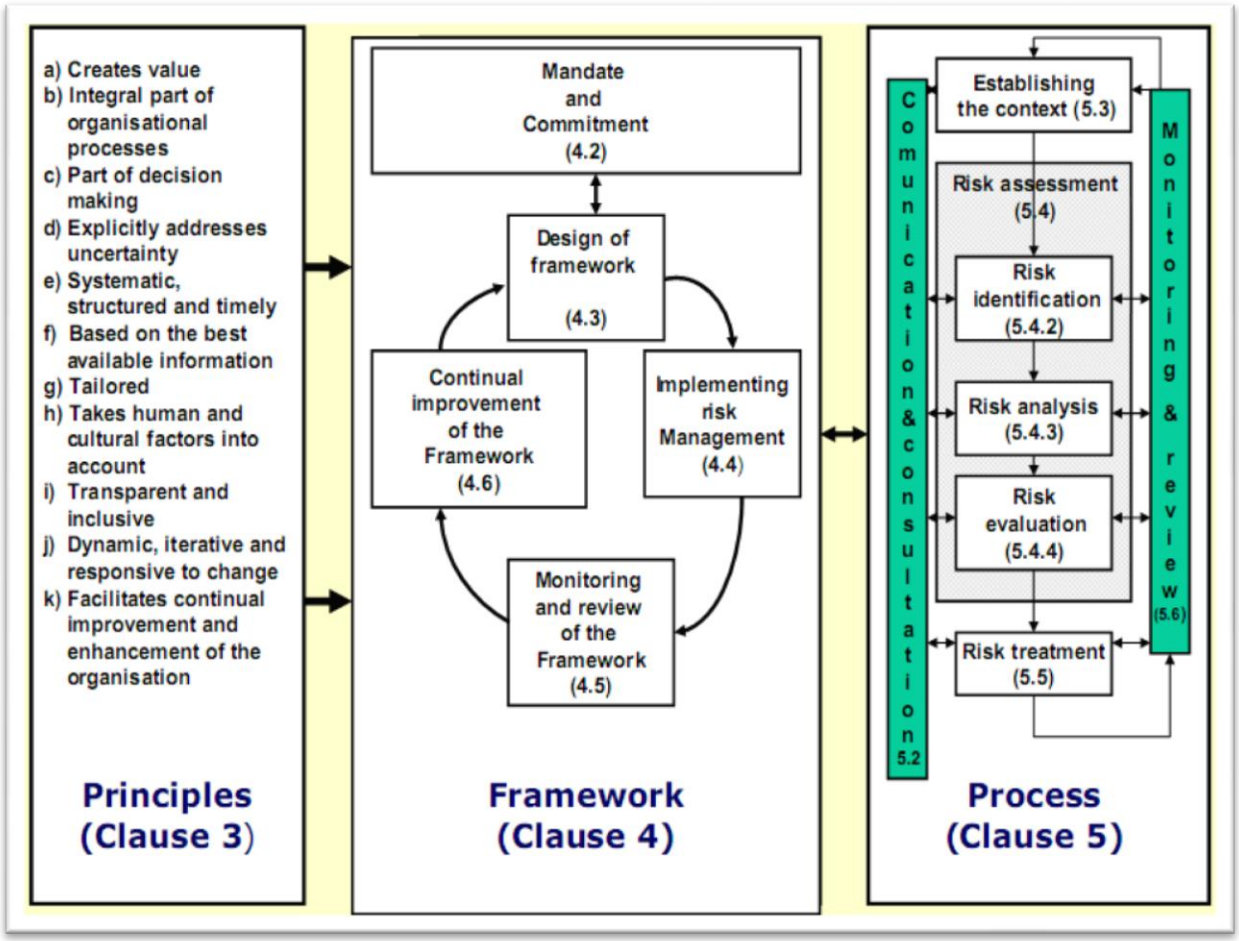
L'ISO 31000 est perçu étant qu'une « norme chapeau » permettant d'établir un dialogue entre les secteurs d'activité en leur proposant un vocabulaire et un cadre commun; elle ne vise pas à promouvoir l'uniformisation des pratiques de management du risque, mais plutôt à harmoniser la myriade d'approches, de standards et de méthodologies existantes en matière de management du risque[2]; de même, sensibiliser les entreprises à l'importance de Risk manager et la nécessité de faire connaître le risque à grande échelle, tant au sein qu'à l'extérieur de l'entreprise; aussi, de renforcer la responsabilisation et la communication du risque.

La norme ISO 31000 est structurée en trois parties, à savoir les principes d'adoption d'un processus de management du risque, cohérents dans un cadre organisationnel « Framework », qui peut contribuer à garantir que le risque est géré de façon efficace, performante et cohérente au sein d'une entreprise ou un organisme. Dont, elle décrit une approche générique pour manager le risque d'une manière systémique, transparente et fiable[3].

La figure ci-après illustre la relation entre les principes, le cadre organisationnel et le processus de management du risque :

[1]AFNOR; The risk culture expressed in ISO 31000; AFNOR certification magazine; Action & Performance 08; La plainte Saint-Denis; France; june 2009; P19-20.
[2]Gilles Motet; La norme ISO 31000 : 10 questions; Les cahiers de la sécurité industrielle; Fondation pour une Culture de Sécurité Industrielle FonCSI; Toulouse; France; 2009. www.icsi-eu.org
[3]ISO/DIS 31000:2009; op.cit; pV.

Figure N°8 : La structure de la norme Risk Management, ISO 31000:2009



Source : ISO/ICE 31000:2009.

Comme le montre la figure ci-dessus, les trois parties structurant la norme ISO 31000 sont comme suit:

- ***Les principes*** répondent à la question pourquoi fait-on de management du risque. Le processus d'intégration de ces principes se fait ensuite à deux niveaux : le niveau décisionnel et le niveau opérationnel.
- ***Le cadre organisationnel*** explique comment intégrer, via le processus itératif de la roue de Deming (Plan-Do-Check-Act), le management du risque dans la stratégie de l'entreprise.
- ***Le processus de management*** précise comment intégrer le management du risque au niveau opérationnel de la stratégie de l'entreprise.

Comme évoqué précédemment, l'ISO 31000 édicte le besoin d'établir des principes au plus haut niveau de management de l'entreprise afin de fournir un engagement réel vers un cadre organisationnel de management du risque. Il s'agit là de prendre en compte l'ensemble des parties prenantes de l'entreprise.

Le cadre organisationnel correspond à un ensemble d'éléments établissant les fondements et dispositions organisationnelles présidant à la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue de management du risque dans toute l'entreprise.

Les fondements incluent la politique, les objectifs, le mandat et l'engagement envers le management du risque. Les dispositions organisationnelles incluent les plans, les relations, les

responsabilités, les ressources, les processus et les activités; il est à noter que le cadre organisationnel de management du risque fait partie intégrante des politiques stratégiques et opérationnelles ainsi que des pratiques de l'ensemble de l'entreprise. D'ailleurs, la norme ISO 31000, constitue une solution efficace pour aider les entreprises à structurer et déployer leur propre approche de risque de façon structurée[1].

Les apports de cette nouvelle norme, permettent d'aborder de façon cohérente et explicite de nombreux aspects interférant généralement de façon anarchique et implicite dans les activités et le processus de management du risque : multiplicité d'objectifs conflictuels, distribution des responsabilités, évaluation de l'efficacité des moyens et de leurs utilisations, etc[2].

Dans le même contexte, dont le mot risque peut désigner une non-conformité en qualité, une pollution en environnement, une défaillance d'un équipement, une atteinte corporelle en matière de sécurité des personnes, aussi un rendement en finance ou une opportunité pour le manager d'entreprise. C'est pourquoi, une révision de vocabulaire de guide ISO/IEC73 a été menée parallèlement aux développements de l'ISO 31000 afin de faciliter les discussions entre tous secteurs. La nouvelle définition enrichit la vision de l'ingénieur « le risque est la combinaison de probabilité d'évènement et de sa conséquence », pour coupler les risques aux objectifs de l'organisation « le risque est l'effet de l'incertitude sur les objectifs »[3].

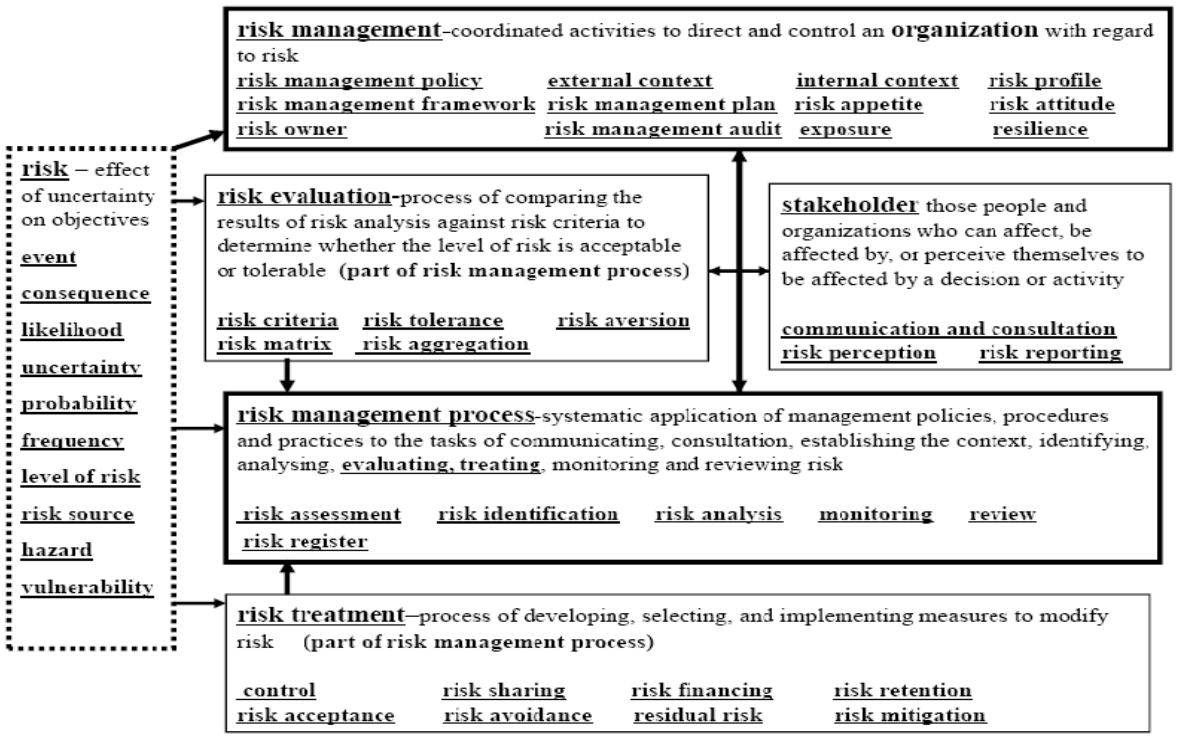
Nous symbolisons sur la figure suivante les principaux termes et typologies figurés sur le référentiel ISO 31000:2009 et le guide 73:2009.

[1]Cecile Agoutin; Management du risque : les enjeux de l'ISO 31000; Publié sur Le cercle des Echos; 17/10/2011; http://lecercle.lesechos.fr/entreprises-marches/management/autres/221138829/management-risque-enjeux-iso-31000 .

[2]Gilles Bernier Ph.D : Professeur de finance & assurance et titulaire de la Chaire Industrielle Alliance; la gestion intégrée des risques : De quoi s'agit-il? ; Conférence organisée par l'AGRAQ-section Québec; Faculté des sciences de l'administration LAVAL; Québec; le 14 juin 2011; P19.

[3]Alex Dali; Les enjeux de la norme ISO 3100 en gestion des risques; La Tribune de l'assurance; N°133; février 2009; p60.

Figure N°9 : les principaux termes de l'ISO 3100 et le Guide 73 :2009



Source: John Shortreed; Risk Management Standard; Ottawa; 2008; p21[1].

Nous allons revenir dans les paragraphes suivants de notre recherche, plus en détails, sur chacun des éléments de la structure de la norme, en clarifiant les termes ci-dessus.

La présente norme ISO 31000 est une avancée importante, soit le premier document international issu d'un consensus sur le management du risque à être largement adopté par plusieurs pays. Cette norme a stimulé l'élaboration de norme parentes: ONR 49000 en Autriche, Q 31001 au Canada, NWA 31000 en Irlande, BSI 31100 en Angleterre, le AS/NZS 4360:2009 qui présente une obligation en Australie et Néo-Zélandais ainsi, le projet AS/NZS HB 436:201X, qui est destiné à aider les parties prenantes à mettre en œuvre la norme[2].

3.3. Comparatifs des principaux standards en matière du « ERM »

Afin de clarifier la problématique de notre recherche aux lecteurs ainsi, faciliter d'avoir une réflexion sur notre démarche, nous proposons ci-dessous une synthèse des principaux référentiels et normes pointus sur le thème de « Entreprise Risk Management ».

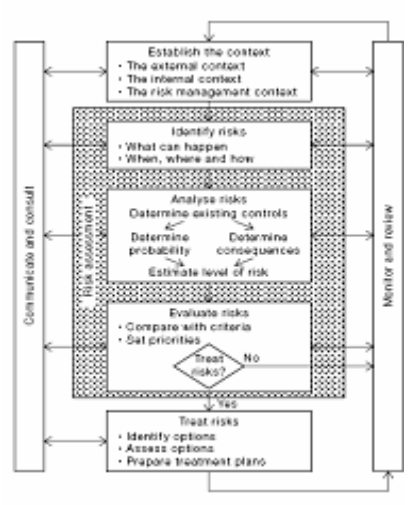
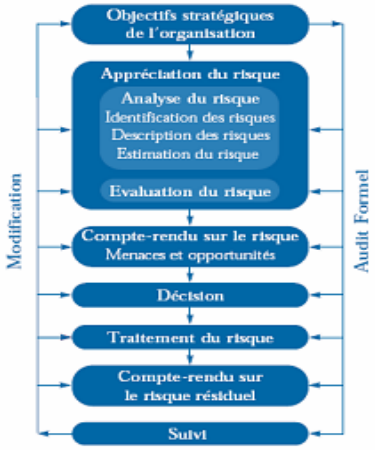
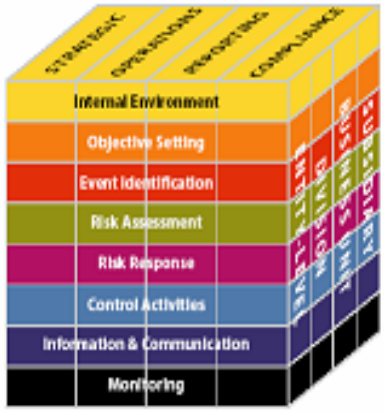
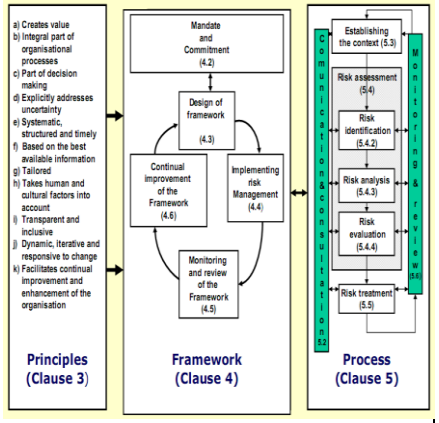
Il s'agit des quatre normes suivantes, du plus ancien au plus récent :

- AS/NZS 4360 : référentiel Australien/Néo zélandais ;
- FERMA : référentiel européen (UK à l'origine) ;
- COSO II : référentiel américain ;
- ISO 31000:2009 : norme internationale

Bien que ces standards n'aient pas de portée obligatoire, ils permettent en général d'obtenir un avantage compétitif.

[1] John Shortreed : Director of IRR; Risk Management Standard; Institute for Risk Research; University of Waterloo; Workshop Ottawa; February 27, 2008; p21.
[2] Kevin W. Knight; La future norme ISO 31000 sur le management du risque; Publication ISO Management Systems; Juillet-Août 2007; p20 ; www.iso.org/ims

Tableau N°4 : Comparatif des principaux référentiels et normes du ERM

Réf	AS/NZS 4360 (1995, 1999 puis 2004)	(FERMA, 2003) (AIRMIC / ALARM / IRM, 2002)	COSO II (2004)	ISO 31000:2009
En résumé	Est le premier standard de Risk Management élaboré en 1995, approuvé par ISO, dont il comporte deux parties : ● les standards de 'ERM'. ● Risk Management guidelines-Companion.	Est, à l'origine, le standard anglais. Représente un document explicatif, détaillé de la terminologie figurée sur le « ISO / Guide 73:2002 ».	Établit un processus générique de MR en huit éléments, présenté par une matrice tridimensionnelle reliant les objectifs organisationnels aux composantes du RM et aux entités d'entreprise.	Constitue un consensus entre plusieurs acteurs et englobe plusieurs normes et référentiels existants. Il incorpore un souci d'uniformisation de vocabulaire autour du risque et d'harmoniser le processus de MR.
QTS	30 pages	14 pages	125 pages	24 pages
Représentation graphique				

La démarche ou le cycle de management du risque	Tout en communiquant et en consultant tout au long du processus, le management du risque suit les quatre étapes suivantes: ● Prise en compte du contexte ● Estimation du risque: ●Identification ●Analyse ●Évaluation ● Traitement du risque ● Pilotage et revue	La démarche du MR comprend les étapes ci-dessous : ● Objectifs stratégique de l'organisation ● Appréciation du risque: ●Analyse (identification, description, estimation du risque) ●Évaluation du risque ● Compte-rendu sur le risque ● Décision ● Traitement du risque ● Compte-rendu sur le risque résiduel ● Suivi	A travers quatre objectifs stratégiques, opérationnels, de reporting et de conformité, le processus RM suit 8 éléments : ● Environnement interne (l'éthiques, la culture du risque, l'appétence pour le risque) ● Fixation des objectifs ● Identification des événements ● Évaluation des risques ● Traitement des risques ● Activités de contrôle ● Information et communication ● Pilotage Ces étapes nécessitent à déployer sur les processus, les filiales, les business unités, les divisions et les entités de l'entreprise.	La démarche de management du risque consiste : ● Le cadre organisationnel décrit le mandat et l'engagement, le contexte et la politique du MR, l'intégration dans les processus d'entreprise... ● La mise en œuvre du processus détaillée par: ●Prise en compte du contexte ●Appréciation du risque ●Identification ●Analyse ●Évaluation ● Traitement du risque ● Surveillance et revue ● Amélioration continue du cadre
Introduction	Introduction similaire à FERMA et COSO II. Met l'accent sur : ● L'importance de l'intégration de la culture du risque dans l'entreprise. ● Le risque comme conséquence de l'incertitude et des écarts potentiels par rapport aux objectifs. ● Le risque peut être une menace et perte, mais également une opportunité et gain.	● Rappelle qu'un cadre de référence de MR, est nécessaire notamment pour préciser : ●La terminologie ●Le processus de déploiement de MR ●L'organisation de MR ●L'objectif de MR ● Se veut un recueil des meilleures pratiques européennes. ● N'a pas vocation à poser les bases d' un processus de certification. ● Pourra servir de base pour démontrer sa conformité. ● Est amené à évoluer à l'avenir.	Fait référence au dispositif de contrôle interne. Exprime l'importance d'avoir : ● Un référentiel global du MR ● Un langage commun ● Un guide d'application Développe le référentiel de contrôle interne mais ne le remplace pas. Illustre de façon d'appréhender le MR dans sa globalité ou bien catégorie d'objectifs, par éléments, par unité ou en les combinant.	Reconnait la diversité de nature, de niveau et de complexité des risques et veut fournir des lignes directrices sur les principes et la mise en œuvre de management du risque. Suggère que certaines directions pourraient revoir leurs pratiques de management à la lumière de cette norme. Rappelle que l'intérêt et l'objectif de MR réside dans la globalité de son application sur tous les domaines de l'entreprise.

Risque, définitions	Définit le risque, comme la résultante de conséquences et d'une probable déviation de ce qui était prévu au départ. Énonce également toutes les autres définitions des termes liés au MR. Les définitions sont dans certains cas propres à la terminologie de l'ISO.	Reprend la norme ISO/IEC Guide73:2002pour définir son risque. Estime que les conséquences de la réalisation d'un risque peuvent être négatives ou positives.	le risque est la possibilité qu'un événement se produise et qu'il ait un effet défavorable sur l'atteinte des objectifs. Démontre que le dispositif du MR comprend les points suivants: ● Aligner l'appétence pour le risque avec la stratégie de l'entreprise. ● Développer les modalités de traitement des risques. ● Diminuer les déconvenues et pertes opérationnelles. ● Identifier et gérer les risques multiples et transverses. ● Saisir les opportunités. ● Améliorer l'utilisation du capital.	Parle de domaines d'application en précisant que la norme est générique. Le risque est effet d'incertitude sur les objectifs.
Le processus du risk management	Idem FERMA Précise que le contexte comprend l'environnement interne et externe à l'entreprise.	Met l'accent sur le MR, qui doit être : ● Intégrée à la mise en œuvre de la stratégie. ● Un processus continu et itératif d'amélioration. ● Partie prenante à la culture de l'entreprise. ● Appropriée par tous les acteurs de l'entreprise. Décrit des facteurs d'origine des risques externes / internes. Catégorise le risque en risque financier, stratégique, opérationnel ou péril.	Explique que le principal défi, pour la direction, réside dans la détermination d'un degré d'incertitude acceptable afin d'optimiser la création de valeur. Prône que la valeur de l'entreprise est maximisée lorsque elle élabore une stratégie (fixe des objectifs) et alloue les ressources nécessaires à l'atteinte des dits objectifs.	Propose 11 principes qui permettront d'optimiser l'efficacité du MR: ● Crée de la valeur et la préserve. ● Intégré aux processus organisationnels. ● Intégré aux processus de prise de décision. ● Traite explicitement de l'incertitude. ● Est systémique, structuré et utilisé en temps utile. ● S'appuie sur la meilleure information disponible. ● Doit être taillé sur mesure et adapté. ● Intègre les facteurs humains et culturels. ● Transparent et participatif. ● Dynamique, itératif et réactif au changement. ● Facilite l'amélioration et l'évolution continue de l'organisme, l'entreprise.

Objectifs	Précise que la description des objectifs est incluse dans la partie « contexte ».	Ne propose pas de partie spécifique afférente aux objectifs même s'il est rappelé l'importance d'adosser les risques aux objectifs stratégiques de l'entreprise.	Est la 2ème composante du référentiel. Demande que les objectifs aient été préalablement définis pour que le management puisse identifier les événements potentiels susceptibles d'en affecter la réalisation. Et que ces objectifs sont en ligne avec la mission de l'entité ainsi qu'avec son appétence pour le risque	Sont intégrés dans la partie « Établissement du contexte » (interne), qui demande également de prendre en compte la culture, l'organisation…, et d'élaborer des critères de risque.
Identification des risques	Décrit l'importance de constituer une liste risques (avec leurs sources et leurs conséquences potentielles) qui pourraient avoir un impact sur l'atteinte des objectifs	Décrit succinctement l'étape qui vise à identifier l'exposition d'une entreprise à l'incertitude. Requiert une approche méthodique pour garantir que chaque activité significative de l'entreprise a été identifiée.	Parle d'événement (interne/externe) au lieu de risque. Soit une opportunité ou une menace. Présente les techniques d'identification et une catégorisation des événements, et évoque la notion d'interdépendance des événements. Propose dans le guide d'application une multitude d'exemples d'identification d'événements.	Décrit l'appréciation du risque comme l'identification, l'analyse et l'évaluation du risque. Cherche à dresser une liste exhaustive d es risques susceptibles d'atteindre les objectifs de l'entreprise. Également du non-saisi d'opportunités.
Documentation du risque	Propose des exemples de risques (dans l e guidelines).	Décrit rapidement la structure de la documentation et propose un exemple de description de risque.	Propose quelques fiches de risques dans la partie guide d'application.	Recherche pour chaque événement possible: les sources (significatives) et les domaines d'impact, ainsi les scenarios à retranscrire dans une documentation.
Estimation du risque	Propose des estimations qualitatives et quantitatives des impacts et de la probabilité ainsi que la nécessité de prendre en compte les contrôles en place.	Énumère très succinctement les techniques qualitatives et quantitatives.	N'existe pas explicitement dans le référentiel.	Parle d'analyse du risque pour décrire l'estimation quantitative, qualitative ou semi-quantitative. Prend en compte les moyens de maitrise ainsi que leur efficacité. Rappelle l'interdépendance qu'il peut y avoir entre certains risques.

Évaluation du Risque	Idem FERMA	Rappelle que l'estimation des risques ne peut suffire et qu'il faut évaluer le risque avec les critères de l'entreprise (coûts et bénéfices associés, contraintes, facteurs socio-économiques et environnementaux.	Parle de risques inhérents et de risques résiduels. Propose des méthodes et techniques qualitatives et quantitatives pour analyser les risques, tant en fonction de leur probabilité que de leur impact.	Vise à déterminer quels risques nécessitent un traitement et un ordre de priorité dans la mise en œuvre du traitement. Rappelle la notion de risque acceptable.
Reporting et Communication	Propose une communication et un reporting constant tout au long du processus du MR.	Suggère une phase de reporting avant de passer à l'étape du traitement.	Après les activités de contrôle, le reporting consiste à communiquer les politiques et procédures déployées afin de veiller l'application des mesures de traitement du risque. Dont, la communication doit circuler verticalement et transversalement au sein de l'entreprise de façon efficace.	Propose une communication et consultation permanente sur toute la mise en œuvre du MR. Recommande une documentation permanente de l'ensemble des activités du MR.
Traitement du risque	Liste les différentes formes de traitement en distinguant le résultat attendu selon qu'il est positif ou négatif. Rappelle la notion de coût/bénéfice. Propose une check-list, (succincte) , à penser pour élaborer un plan de traitement.	Propose un paragraphe succinct rappela nt que le traitement du risque a pour principales composantes la maîtrise et l'atténuation du risque mais ne s'y limite pas et parle d'évitement, de transfert ou de financement.	Énonce les quatre formes de traitement durisque : évitement, réduction, partage, acceptation ainsi que l'implication du traitement dans le coût/bénéfice, le seuil de tolérance et l'appétence pour le risque d'entreprise. Distingue la composante des activités d e contrôle du traitement des risques.	Implique un processus itératif d'appréciation du traitement du risque , qui vise à décider si les niveaux résiduels de risques son tolérables ou non. Propose un panel de plusieurs options d e traitement pas nécessairement mutuellement exclusif. Ènumère les informations nécessaires à lamise en œuvre d'un traitement de risqu
Pilotage et revu e	Indique que le contrôle permanent du processus est essentiel et se réalise en analysant les événements, leurs plans d'actions et les résultats finaux.	Préconise un audit régulier du processus permettant de fournir une assurance que le dispositif de maîtrise est approprié.	Préconise une revue permanente de l'efficacité du processus en interne et une revue spécifique par des auditeurs internes ou une entité indépendante.	Préconise une revue régulière notamme nt de l'avancement des plans de traitement. Recommande la documentation des revues interne ou externe.

Source : préparé par l'étudiante et inspiré essentiellement de l'ouvrage de Bénédicte H.L[1], ainsi que les documents des quatre référentiels.

[1]Bénédicte Huot de Luze; Comparatif des référentiels de gestion des risques; Dossiers de la newsletter AMRAE; Décembre 2009; p 2-10.

Comme le montre le comparatif ci-avant, nous retiendrons que ces quatre principaux référentiels, donnent des cardes utiles pour l'intégration efficace du management du risque dans l'entreprise. Ils ont des caractéristiques communes, sur les points suivants :

- Désignent un processus générique de management du risque tout en préconisant de la flexibilité dans le déploiement.
- Sont applicables à structure d'organisations et d'activités très diverses.
- Conviennent que le management du risque est une bonne pratique de management qui doit se fondre et intégrer dans le processus de l'entreprise.
- Recherchent les menaces mais également les opportunités.
- Définissent leur propre terminologie pour permettre une meilleure compréhension de concepts.

En effet, le standard Australien et l'ISO 31000 ont des similitudes au niveau de leur approche. Ils abordent la notion de management du risque d'une manière générale. Dont, le COSO II se veut être plus détaillé et tourné davantage vers l'application du processus de management du risque fondé sur le contrôle interne et l'audit. Cela peut expliquer par les experts qui rédigent ces documents, l'ISO et le standard australien étant écrit par des experts du Risk Management, tandis que le COSO II, est le fruit des spécialistes de l'audit et contrôle interne.

Le référentiel du FERMA (AIRMIC/ ALARM / IRM), fournit un document explicatif de la terminologie présentée dans la norme ISO/IEC 73 :2002 intitulée par Risk Management-Vocabulary. Dont en 2010, cette association européenne de management du risque, a publiée un autre référentiel fondé sur l'approche Entreprise Risk Management proposée sous l'ISO 31000:2009.

Notant que l'ISO 31000 permet d'aboutir à une convergence potentielle entre une méthodologique normative et une méthodologique réglementaire, celle du COSO.

De manière générale, chacun de ces standards a ses propres attributs et aucun n'est nécessairement meilleur que l'autre. Toutefois, quelque soit le standard adopté, il est important qu'il soit adapté correctement pour refléter la complexité de l'entreprise.

Dans ce contexte, et afin de mieux cerner notre problématique, notre démarche constitue un prolongement des réflexions de ces référentiels, essentiellement du COSO II et la norme ISO 31000 la version 2009 du ISO et 2010 celle de AFNOR et de AIRIMIC; dont, la norme ISO 31000 rejoint le COSO II sur plusieurs points, tel que : l'appétence au risque « Risk appetite », le positionnement du risque dans la structure d'entreprise, ainsi les responsabilités et les objectifs de l'entreprise. Nous verrons plus amples de détails sur les déférents volets de ces standards en développant notre recherche.

Au-delà de l'harmonisation des processus de management du risque que la norme ISO 3100 est susceptible d'apporter, l'enjeu porte aussi sur la profession du Risk Manager, pour qui l'apparition d'un standard international est un gage de crédibilité. En faite, la fonction s'en trouve mieux structurée, plus préparée à maîtriser l'évolution générale de la complexité de l'environnement de l'entreprise.

Toutefois, l'Autorité des Marchés Financiers a publiée un cadre de référence, qu'il a été réactualisé en 2010, traite à la fois du contrôle interne et de management du risque. Ce cadre n'est pas obligatoire mais constitue indéniablement une bonne pratique pour mettre en œuvre la loi du 3 juillet 2008. Cette loi transpose en droit française la 4ème et la 7ème directive européenne qui obligent toutes les sociétés cotées à fournir dans leur rapport de gestion une information sur ses principaux dispositifs de contrôle interne et de management du risque. Il s'inspire notamment du COSO-II et de la norme ISO 31000.

Section 3 : L'implantation et le développement d'une approche globale de Risk Management au sien de la structure de gouvernance d'entreprise

Le management des risques est de plus en plus reconnu comme l'une des composantes essentielles d'une bonne gouvernance. Des pressions s'exercent sur les organisations pour identifier les risques significatifs auxquels elles sont confrontées, les risques sociaux, déontologiques et environnementaux, mais aussi les risques stratégiques, financiers et opérationnels, et expliquer comment elles les gèrent et managent. L'adaptation de cadres de management du risque à l'échelle de toute l'entreprise se développe au fur et à mesure que les organisations prennent conscience des avantages d'approches coordonnées.

La construction d'un dispositif de risk management mature nécessite de développer une approche progressive et pragmatique. Vouloir tout couvrir en une seule fois est illusoire et inefficace. Il faut bien cerner les enjeux majeurs et les zones à risque pour mettre en œuvre les dispositifs adaptés à chaque groupe, qui seront améliorés.

La présente section de notre recherche s'appuie sur la norme ISO 31000 afin de définir les grandes lignes du cadre organisationnel de management du risque, ainsi, d'autres référentiels, telle que le cadre du COSO-II, peuvent être utilisés pour enrichir l'objet de cette section. Nous proposons ci-après une trame méthodologique d'intégration de management du risque dans les processus organisationnel de l'entreprise.

1. Le modèle conceptuel du cadre organisationnel d'ERM

Comme nous l'avons énoncé précédemment, l'approche globale d'Enterprise Risk Management favorise une démarche systémique, continue et proactive visant à comprendre, surveiller, gérer, maîtriser et communiquer les risques du point de vue de l'ensemble de l'entreprise d'une manière cohérente et structurée.

D'ailleurs, la norme ISO 31000 décrit que « *le succès de management du risque dépend de l'efficacité du cadre organisationnel de management qui fournit les bases et les dispositions permettant son intégration à tous les niveaux organisationnel*[1]».

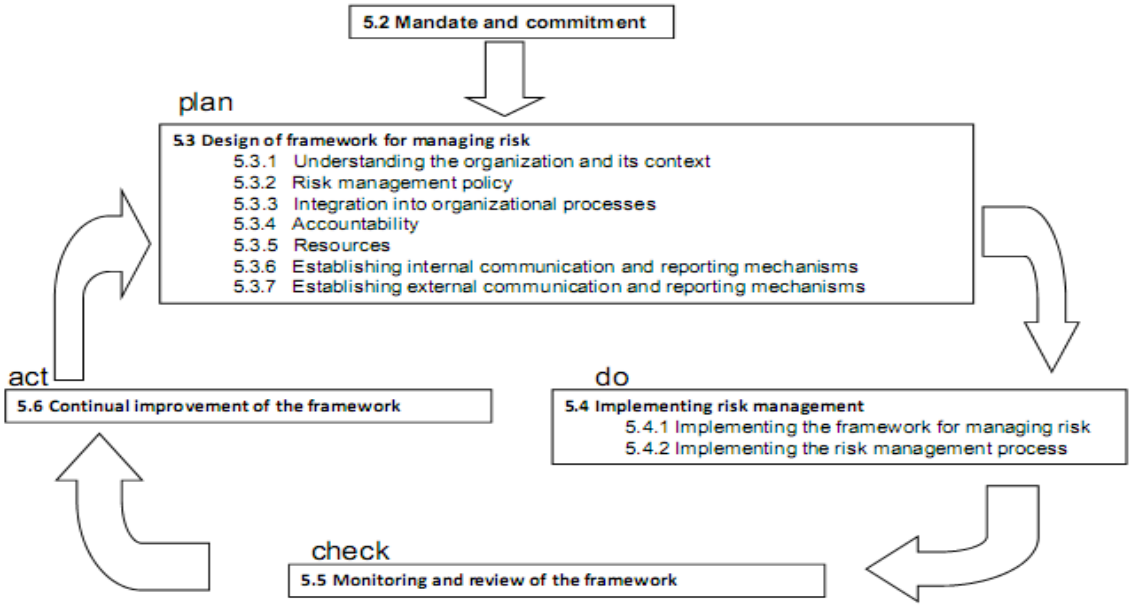
Toutefois, au lancement d'une démarche de management du risque, en amont de sa mise en place, la haute direction de l'organisation doit décider de l'approche qu'elle envisage pour appliquer le référentiel adéquat à sa complexité, sa activité, son style de management.

En effet, La norme ISO 31000 fournit des orientations pour structurer le management du risque au sein d'une entreprise. Elle définit le cadre comme un « *ensemble de composantes établissant les fondements et les dispositions organisationnelles nécessaires à la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue de management du risque dans tout l'organisme*[2]». Quel que soit son niveau de formalisation, le dispositif de management du risque est intrinsèquement intégré dans les politiques stratégiques et opérationnelles ainsi que dans les pratiques de l'entreprise. Les dispositions organisationnelles incluent les projets, les interactions, les responsabilités, les ressources, les processus et les activités.

La figure ci-dessous présente la relation entre les composantes du cadre organisationnel de management du risque proposé par la norme ISO 31000.

[1] ISO/FDIS 31000; op.cit ; p9.
[2] ISO/IEC guide 73 ; op.cit ; p2.

Figure N°10 : Le cadre organisationnel d'Enterprise Risk Management selon l'ISO 31000



Source : ISO/DIS 31000 : 2009 ; p3.

Ce cadre n'est pas destiné à prescrire un système de management mais plutôt à aider les entreprises ou les organismes en général, à intégrer le management du risque dans son système de management global. En autre, la norme ISO 31000 précise que le cadre est conçu pour être adapté aux besoins et à la structure propre à chaque entreprise.

Il est aisé de constaté, à la lumière de ce qui précède, que le cadre organisationnel est constitué d'un cycle de type PDCA « *Plan, Do, Check & Act* » bien connu sous la roue de Deming. Il commence par une phase de conception, puis de mise en œuvre, d'exécution et clôture la boucle par d'amélioration de la démarche de management du risque au sein de l'entreprise.

Le cadre organisationnel de management du risque est axé sur deux principaux volets: ***l'approche globale de management du risque*** reflétant la démarche d'intégration de management du risque au sein d'une organisation, et ***le processus de management du risque,*** les étapes permettant de gérer le risque de manière cohérente.

Comme nous l'avons déjà évoqué le modèle conceptuel du cadre organisationnel proposé par la norme ISO 31000 inclus les composantes de management du risque décrit par le référentiel COSO-II aussi bien les dispositions relevant des lois Sarbanes-Oxley et LSF.

1.1. Engagement et conception du cadre organisationnel de management du risque

L'implication de la haute direction de l'entreprise dans la démarche de conception du cadre organisationnel de management du risque constitue un point de départ indispensable pour lancer le projet de développer et de renforcer une approche progressive et pragmatique d'un cadre efficace et durable. Il s'agit d'apprécier la volonté et la capacité nécessaire pour mettre en place les outils et opérer les changements nécessaires, introduisant le management du risque aux structures courantes de gouvernance et d'organisation d'entreprise.

Il est à noter que cette phase reflète *l'environnement interne* décrit sous le cadre COSO-II, qui constitue le fondement structurel sur le quel peuvent s'appuyer tous les autres éléments ou composantes d'Enterprise Risk Management.

D'un coté, l'environnement interne exerce une influence sur la façon dont la stratégie et les objectifs son définis, sur la façon dont les activités sont structurées et la manière dont les risques sont surveillés et maîtrisés; également il a une influence sur la conception et le fonctionnement des activités de contrôle, sur les systèmes d'information et de communication ainsi sur le suivi des opérations.

D'un autre coté, l'environnement interne est influencé par l'histoire et la culture de l'organisation; il englobe l'intégrité, les valeurs éthiques, la culture de l'organisation en matière de management du risque, son appétence pour le risque, la surveillance exercée par le conseil d'administration ou la haute direction, la compétence du personnel, la politique de délégation de pouvoirs et de responsabilités, l'organisation et le développement des collaborateurs[1]. Aussi bien, la conception du cadre tient en compte la *fixation des objectifs* stratégiques, opérationnel, de reporting et de conformité, alignés sur l'appétence de l'organisation pour le risque et sa tolérance au risque.

Mandat et engagement « Mandate & commitment »

Certes, la construction d'un dispositif de risk management mature au sein d'une entreprise ne passe pas uniquement par le déroulement d'une méthodologie structurée. Dont, l'introduction de management du risque et l'assurance de son efficacité permanente exigent un appui et un engagement officiel, fort et durable de la direction et des acteurs de la gouvernance de l'entreprise; ainsi que l'établissement d'un plan stratégique rigoureux pour construire un engagement à tous les niveaux organisationnels.

Il faut reconnaitre dès le départ que la construction et l'intégration d'une approche globale de management du risque implique un changement culturel important en passant d'une approche verticale à une autre plus horizontale[2]; pour ce faire, la direction doit s'assurer l'engagement et concordance avec les autres autorités de gouvernance d'entreprise.

Dans cette perspective, en amont de la mise en place du cadre organisationnel de management du risque, la direction doit décider de l'approche qu'elle envisage pour appliquer le référentiel adapté à l'ensemble de l'organisation. Les travaux menés dans le cadre de COSO-II, montre que les organisations au sein desquelles le management du risque a été mis en œuvre avec succès présentent un certain nombre de points communs comme suit[3] :

- ***Mise en place d'une équipe centrale*** : La création d'une équipe centrale, composée de représentants de chaque unité opérationnelle et des principales fonctions support, y compris la planification stratégique. Cette équipe doit maîtriser les éléments, concepts et principes du cadre référentiel adapté, afin concevoir et déployer un dispositif de management du risque répondant au mieux aux besoins propres de l'entreprise ;

- ***Parrainage de la direction*** : L'implication de la direction signale l'engagement de l'organisation, et leur appui soutenu est déterminant pour la réussite de la mise en œuvre de management du risque. il revient à la direction d'expliciter les bénéfices liés au management du risque, et également d'établir et de communiquer sur les ressources qui y sont affectées ;

- ***Développement du plan de mise en œuvre*** : Un premier plan est établi, définit les différentes phases et décrit les principales étapes du projet d'implantation de management du risque incluant les travaux, jalons, ressources et calendrier; ainsi détermine les responsabilités. Ce plan constitue un moyen de communication et de coordination avec

[1] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 40.
[2] Secrétariat du Conseil du Trésor de Canada SCT; Gestion intégrée du risque : Guide de mise en œuvre ; STC; Canada; 2004; p 9. Disponible sur le lien www.tbs-sct.gs.ca
[3] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 160-161.

les responsables du projet de mise en œuvre; il est utilisé pour discuter et valider la prise en compte de leurs attentes avec les unités et membres du personnel aussi bien ce plan sert également à discuter les changements à mettre en place à l'échelle de l'organisation préalablement à l'adoption du dispositif de management du risque ;

➲ ***Évaluation de la situation existante*** : Il s'agit d'évaluer la manière dont sont appliqués les éléments, concepts et principes de management du risque au sein de l'organisation. Cela consiste à assurer qu'une culture de management du risque s'est développée et à déterminer si l'appétence pour le risque est uniformément compris. L'équipe centrale identifie également les politiques, processus, pratiques et techniques actuellement en place, ainsi les compétences présentes au sein de l'organisation ;

➲ ***Vision du management du risque de l'organisation*** : L'équipe centrale met au point une vision qui détermine la manière dont le mangement du risque sera intégré et mis en œuvre au sein de l'organisation. Cette vision permet de orienter les efforts de l'organisation en vue de mettre en adéquation l'appétence pour le risque avec la stratégie, de renforcer les décisions en matière de traitement des risques, d'identifier les risques transversaux, d'évaluer les opportunités et d'améliorer l'affectation des ressources et capitaux ;

➲ ***Développement des compétences :*** L'évaluation de la situation actuelle de l'organisation et l'élaboration d'une vision du management du risque donnent les informations nécessaires en vue de déterminer, d'une part, les acquis en matière de compétences, de processus et de technologie et, d'autre part, quels sont les éléments qui doivent être renforcés et développés. Cela conduit notamment à définir les rôles et responsabilités ainsi que les changements ou les modifications à apporter au modèle organisationnel, aux politiques, aux processus, aux méthodologies, aux outils, aux techniques, aux flux d'information et aux technologies ;

➲ ***Plan de mise en œuvre :*** En général, ce plan couvre les étapes traditionnelles de gestion de projet que l'on retrouve dans tout processus de mise en œuvre. Dont, il doit être mise à jour et enrichi afin de pouvoir continuellement déterminer les déploiements complémentaires du processus de mise en place de management du risque ;

➲ ***Gestion du changement :*** Des actions sont initiées autant qu'il est nécessaire afin de contribuer à la mise en œuvre de la vision d'organisation en matière de management du risque et des compétences souhaitées. Ces actions intègrent souvent des plans de déploiement, des sessions de formation, de sensibilisation aux risques, des mécanismes de rétribution ainsi que le pilotage du processus de mise en œuvre ;

➲ ***Pilotage :*** Le management devra examiner et renforcer continuellement les compétences en matière de management du risque dans le cadre de ses attributions courantes.

Il est à noter que le choix d'internaliser ou d'externaliser le projet de mise en œuvre de management du risque au sein de l'organisation n'est pas sans incidence ni risques. Tout internaliser « équipe centrale interne, tel que le comité du risque » permet d'impliquer les opérationnels dans la mesure où le responsable du projet a le poids suffisant dans la hiérarchie; le risque induit présente une difficulté à identifier les bonnes pratiques qui ne seraient pas en place dans l'organisation.

Toutefois, l'externalisation complète du projet de mise en œuvre de management du risque n'est pourtant pas conseillée. Le risque de désappropriation par l'équipe interne est très élevé; une fois les consultants partis, le dispositif de management du risque s'étoile et n'est plus maintenu, alors que les risques et les processus critiques sont toujours présents.

Bien entendu, il est favorable de constituer une équipe interne, trouver le meilleur accompagnement externe par des cabinets spécialisés avec des outils appropriés et de benchmark de ce qui se pratique ailleurs[1].

De même, cette mise en œuvre de dispositif de management du risque est un projet à moyen ou à long terme qui requiert un horizon de planification s'échelonnant sur plusieurs années. La rapidité de la mise en œuvre de ce dispositif dépend largement de la culture de risque et de la structure de l'entreprise en question. Les organisations qui ont réussi à instaurer une culture de risque à tout l'échelon de l'entreprise ont été en mesure de raccourcir la durée de l'intégration du dispositif, tandis que, celles ayant une structure organisationnelles et hiérarchique complexe ont tendance à y consacrer plus de temps[2].

Conception du cadre organisationnel de management du risque « Design of framework for managing risk »

La conception d'un cadre efficace de management du risque au sein d'une entreprise passe par certaines phases à accomplir :

- Acquérir une compréhension de l'organisation et de son contexte afin de relever les facteurs susceptibles d'avoir une incidence importante sur la conception de l'approche et du processus de management du risque ;
- Formuler un énoncé de la politique de management du risque propre à l'entreprise et approuvé par la haute direction ;
- Définir un processus uniforme de management du risque comprenant une terminologie commune ;
- Définir les responsabilités en matière de management du risque ;
- Affecter les ressources nécessaires à la mise en œuvre et au soutien de management du risque au sein de l'entreprise ;
- Définir des mécanismes de communication et de production de rapports.

Compréhension de l'organisation et de son contexte « Understanding the organization and its context »

Préalablement à la conception et à la mise en œuvre du cadre organisationnel de management du risque, il est important d'évaluer et de comprendre le contexte tant interne qu'externe de l'entreprise, étant donné que celui-ci peut influencer la conception du cadre de façon significative le faite que la tolérance au risque d'une entreprise varie en fonction de sa culture et des conditions changeantes de son environnement interne et externe.

➢ L'évaluation du contexte interne de l'entreprise peut se pencher sur les éléments suivants :

- La gouvernance, l'organisation, les rôles et les responsabilités ;
- Les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers ;
- Les aptitudes, en termes de ressources et de connaissances telles que le temps, personnels, processus, systèmes et technologies ;
- les systèmes d'information, les processus de prise de décision à la fois formels et informels ;

[1] Pascal Kerebel ; op.cit ; p52-53.

[2] Towers Perrin. A Changing Risk Landscape: A Study of Corporate ERM in the U.S. http://www.towersperrin.com/tp/getwebcachedoc?webc=HRS/USA/2006/200611/ERM_Corporate_Survey_110106.pdf publié dans institut canadien des actuaires , actuaires CA ; p 8

- Les relations avec les parties prenantes internes, leurs perceptions et leurs valeurs, ainsi que la culture de l'entreprise ;
- Les normes, lignes directrices et modèles adoptés par l'entreprise ;
- La forme et l'étendue des relations contractuelles.

➢ L'évaluation du contexte externe de l'entreprise peut comprendre, entre autres :

- L'environnement social et culturel, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local ;
- Les facteurs et tendances ayant un impact déterminant sur les objectifs de l'entreprise ;
- Les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

● ***Établissement de la politique de management du risque « RM policy »***

La politique de management du risque précise l'orientation générale de l'entreprise en matière d'intégration des risques, dont sa vision, sa stratégie, ses objectifs et sa culture. Au moment d'énoncer et d'articuler son orientation vers l'intégration de management du risque, l'entreprise devrait prendre en considération les éléments suivants:

- Les motivations de l'entreprise en matière de management du risque ;
- La cohérence de la politique et les objectifs de management du risque avec les orientations stratégiques de l'entreprise ;
- Les responsabilités nécessaires au management du risque ;
- La manière de gérer les intérêts contradictoires ;
- L'engagement à assurer les ressources adéquates pour le management du risque ;
- Le mode d'évaluation du rendement et les performances de management du risque, les modalités de suivi de son qualité et son audit, ainsi les rapports de communication sur son efficacité ;
- L'engagement à revoir et à améliorer la politique et le cadre organisationnel de management du risque périodiquement et à la suite d'un événement ou d'un changement de circonstances ;
- Les principales orientations de réduction et de financement du risque et notamment les dispositifs de plan de continuité d'activité et de management de crise.

Catherine & Richard décrit qu'il n'y a pas de management du risque efficace sans politique générale clair de ce dernier, d'objectifs formels et de plans d'actions quantifiés et planifiés. C'est la combinaison et la pondération des déférents ordres d'objectifs techniques, réglementaires, économiques et humains, etc, qui définit l'équilibre recherché par l'entreprise et qui caractérise in fin la politique de management du risque[1].

La politique générale de management du risque comporte principalement les points ci-dessous :

➲ ***Un périmètre et une période de référence :*** Le périmètre est constitué des activités de l'entreprise couvertes par la politique. La période de référence est généralement annuelle. Autrement dit, la politique de management du risque est passée en revue et mis à jour chaque année ou en cas d'un événement rebouteux ;

➲ ***Un langage commun :*** afin de s'assurer la cohérence de mise en œuvre de la politique de management du risque au sein de l'entreprise par les personnes concernés et la

[1] Catherine Véret et Richard Mekouar ; op.cit ; p60.

participation active de toute la pyramide des responsables, il est nécessaire d'utiliser un langage commun de manière à partager les mêmes principes, référentiels et méthodes ;

➲ ***Des personnes identifiées responsables de l'application de la politique :*** le risk Manager ou le directeur de Risk management (ou son équivalent) à la responsabilité d'orchestrer la politique de management du risque. il rend compte aux dirigeants de l'entreprise. Dans tous les cas, le risk manager n'est pas le seul acteur de la mise en œuvre de management du risque, une chaîne de responsabilités est construite en impliquant toute l'entreprise. En effet, comme nous avons déjà vu, la construction d'une architecture de management du risque nécessite souvent la mobilisation d'une équipe ad hoc et de groupe de travail supervisés par un comité de pilotage, le tout animé par le risk manager ;

➲ ***Une démarche solide de mise en œuvre :*** une politique générale de management du risque doit être à la fois simple et applicable. Elle définit les objectifs, les actions envisagées ainsi les rôles et les responsabilités en chacun; de même, la politique s'appuie sur la démarche du risk manager qui précise également les critères d'appréciation de tolérance aux risques retenus par l'entreprise et les paramètres fondamentaux pour leur évaluation ;

➲ ***Un processus de suivi et de contrôle :*** il est décisif que la politique de management du risque soit accompagnée de dispositifs assurant le suivi de la bonne application de celle-ci. Cela suppose des processus spécifiques systématiques et communs à l'ensemble de l'organisation pour l'évaluation, le reporting, l'audit et le contrôle.

- ***Intégration aux processus organisationnels «Integration into organization processes »***

L'un des facteurs déterminant pour le succès de la conception et la mise en œuvre est l'intégration homogène de management du risque à toutes les pratiques et tous les processus de l'organisation de façon à être pertinent, efficace et performant; notamment que le management du risque soit pris en compte dans la planification et l'élaboration de la politique, les plans d'activité et stratégiques et leur revue, et dans les processus de management du changement.

Comme évoqué par Lucienne Robillard[1], le management efficace du risque ne se pratique pas en vase clos ou en silos il doit être intégré aux structures et aux processus décisionnels, soit au management stratégique et d'exploitation assurant que le management du risque fait partie intégrante des activités quotidiennes.

Lucienne décrit que chaque entreprise ou organisation doive trouver la méthode qui lui convient pour intégrer le management du risque à ses structures existantes de prise de décisions; bien que l'entreprise doit améliorer les systèmes et processus de contrôle et de responsabilisation afin de tenir compte de management du risque et des résultats y afférents.

- ***Responsabilités « Accountability & authority »***

Comme on l'a énoncé ci-avant, la haute direction doit s'assurer la mise en œuvre de management du risque au sein de l'entreprise, ainsi l'adéquation des responsabilités, l'autorité et les compétences appropriées, y compris d'assurer la qualité, l'efficacité et la performance de tous moyens de maîtrise du risque. Dont, l'entreprise devrait tenir compte des aspects suivants :

- Désigner adéquatement les propriétaires du risque à qui incombe la responsabilité et l'autorité de gérer les risques ;

[1] Lucienne Robillard, la présidente du Conseil du Trésor de Canada; Cadre de gestion intégrée du risque; Conseil du Trésor de Canada; Avril 2001; p 22-23. Disponible sur le site www.tbs-sct.gs.ca

- Faire en sorte que les structures de gouvernance de l'entreprise permettent les niveaux de responsabilisation et d'autorité nécessaires pour les responsables des risques ;

- Désigner l'entité appropriée pour l'élaboration, la mise en œuvre et le maintien du cadre de management du risque ;

- Mettre en place les mécanismes de mesure de performance ainsi que les processus de rapports et de recours hiérarchiques internes et externes ;

- Établissement de niveaux opportuns de reconnaissance, de récompenses, d'approbation et de sanction ;

- ***Ressources « Resources »***

Il faut affecter les ressources adéquates à la conception, à la mise en œuvre et à l'amélioration du cadre de management du risque de même qu'à la réalisation continue des activités liées à la maîtrise des risques.

Il est possible que des coûts de démarrage (temps, sensibilisation, formation, systèmes d'information et communications) soient engagés jusqu'à ce que la pratique devienne une partie intégrante des structures et des processus organisationnels. Il faudra probablement du temps et des efforts pour donner une impulsion à l'initiative, pour former les manager, les gestionnaires et les spécialistes et pour mettre en place les bons outils et les bons processus. Les investissements initiaux pourront être réaffectés selon les besoins une fois la mise en œuvre complétée.

Pour évaluer les ressources nécessaires de management du risque, il est important de déterminer la nature, la pertinence et l'utilité des outils, des techniques, des compétences et du savoir-faire afin de définir les besoins supplémentaires. Les considérations liées aux ressources pourraient comprendre, sans s'y limiter :

- Les personnes, les compétences, les attitudes, l'expérience ;

- Les processus, les méthodes, les outils organisationnels, les systèmes d'information servant au management du risque;

- Les programmes de formation nécessaires à l'intention du personnel de l'entreprise pour assurer une compréhension, une approche, langage et terminologie communes de management du risque.

- ***Établissement de mécanismes de communication et de rapports internes et externes « Internal & external communication & reporting »***

La communication des risques au moment opportun fait partie intégrante du processus de prise de décision. Pour ce faire, il faut communiquer l'information sur le risque à l'intérieur de l'entreprise d'une manière utile et efficace, de même qu'à l'extérieur aux clients et aux parties intéressées susceptibles d'intervenir dans les décisions et les actions de l'entreprise ou d'en subir les répercussions. Afin de parvenir à une communication efficace des risques, il est important, dans la mesure du possible, de fournir à chacun toute l'information nécessaire pour contribuer de manière éclairée au processus de prise de décision.

Il existe divers outils et techniques pour communiquer l'information sur le risque, c'est pourquoi il serait opportun d'établir un mode unique de communication du risque au sein d'une entreprise, tels que les tableaux de bord et les profils de l'organisation, des secteurs ou des divisions peuvent donner la possibilité de communiquer efficacement les risques

importants à l'échelle de l'entreprise d'une manière régulière, permettant ainsi d'établir des liens entre les risques touchant les programmes, les projets, les processus, etc[1].

Il convient que ces mécanismes de communication sur les risques, garantissent ce qui suit :

- Consultation des parties intéressées internes et externes pour concevoir le cadre de management du risque ;

- Communication de l'engagement et de la vision de la haute direction en matière de management du risque dans l'ensemble de l'organisation ;

- Production de rapports sur l'efficacité et les résultats de l'approche et le processus de management du risque ;

- Communication des bonnes pratiques et des leçons tirées et mise au point concertée de ressources sur le risque pour l'amélioration continue des processus ;

- Établissement de rapports externes conformes aux obligations légales, réglementaires et aux exigences de la gouvernance de l'entreprise ;

- L'utilisation de la communication pour renforcer la confiance des parties prenantes, notamment en cas de crise.

1.2. Mise en œuvre de management du risque « Implementing risk Management »

Une fois le cadre organisationnel du management du risque conçus, incluant l'approche adaptée et le processus d'application systémique de la politique, les procédures et les activités de maîtrise des risques; il faut les mettre en œuvre prenant en considération ce qui suit :

Mise en œuvre du cadre organisationnel de management du risque

La mise en œuvre du cadre organisationnel de management du risque exige que la stratégie globale de maîtrise des risques soit appliquée dans l'ensemble de l'organisation conformément à l'approche établie. Lorsqu'une approche de management du risque est déployée au sein d'une organisation, il faut envisager exécuter les activités suivantes :

- Définir un calendrier et une stratégie appropriés pour la mise en œuvre du cadre organisationnel de management du risque en conformité à la politique et aux obligations légales et réglementaires ;

- Assurer que les prises de décision, y compris l'élaboration et la détermination des objectifs, sont cohérentes avec les conclusions des processus de management du risque ;

- Fournir aux membres du personnel la formation et les moyens pour apprendre à connaître et mieux comprendre l'approche organisationnelle de management du risque ainsi que leurs rôles et responsabilités ;

- Communiquer et de concerter avec les parties prenantes afin de s'assurer que le cadre organisationnel de management du risques reste approprié.

Mise en œuvre du processus de management du risque

Au sens large, le processus de management du risque se définit comme une série d'étapes interreliées et interdépendantes qui peuvent être réitérées et vérifiées. Ils offrent une structure permettant de systématiquement relever, évaluer, résoudre, communiquer et surveiller les risques significatifs dans une structure de gouvernance établie. En plus de faciliter les décisions quotidiennes à l'échelle individuelle, ces mécanismes permettent acquérir une vision

[1] Secrétariat du Conseil du trésor du Canada; Guide de gestion intégrée du risque : Approche recommandée pour la préparation d'un profit de risque organisationnel; STC; Canada; 2010. Disponible sur le site www.tbs-sct.gs.ca

stratégique et globale des risques importants à l'échelle organisationnelle nécessitant une attention soutenue de la haute direction de toute l'entreprise.

Une fois défini, le processus de management du risque pourra servir à réaliser des évaluations concrètes des risques et s'intégrer aux structures et processus en place afin de favoriser une prise de décisions éclairée par l'analyse des risques pertinents.

Le processus de management du risque permet l'application systémique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identifications, d'analysa, d'évaluation, de traitement, de surveillance et de revue des risques; ce qui permet d'acquérir un certain niveau d'assurance quant à l'atteinte des objectifs et des résultats attendus[1].

Comme c'est le cas pour l'approche de management du risque, le processus de gestion du risque devrait refléter la culture et les procédés organisationnels ainsi que les intérêts de l'ensemble des parties prenantes de l'entreprise. Le fait de tenir compte de ces facteurs dans la conception de l'approche globale facilitera l'élaboration et la mise en œuvre du processus de management du risque. Cette façon de faire permet de donner le ton aux niveaux supérieurs et d'accroître la mobilisation et le consensus aux niveaux stratégiques et opérationnels.

Nous présenterons plus amples de détails sur le processus de management du risque dans le deuxième chapitre de notre recherche.

1.3. Surveillance, revue et amélioration continue du cadre organisationnel d'ERM

La surveillance et la revue sont des aspects cruciaux de l'amélioration continue du cadre organisationnel du management du risque, ils sont essentiels au maintien de l'efficacité et de la pertinence de la démarche de maîtrise des risques quant au soutien de la performance globale de l'entreprise.

Les commentaires, les observations et les recommandations rassemblés au fil des activités de surveillance et de revue permettent à l'entreprise de déterminer si l'approche et le processus de management du risque donnent les résultats escomptés ainsi que de relever les lacunes, manques d'efficacité et occasions d'amélioration éventuels.

Surveillance et revue du cadre organisationnel « Monitoring & review of the framework »

Cette phase du cadre organisationnel impose la construction d'indicateurs de performance permettant de monitorer la montée en puissance de la maturité du dispositif de management du risque et d'effectuer régulièrement des revues de performance[2].

En faite, la surveillance inclus la supervision, la détermination et l'identification continûment des changements par rapport au niveau de performance exigé ou attendu; dont, la revue se focalise sur l'adaptation, l'adéquation et l'efficacité du cadre organisationnel du management du risque[3].

Afin de s'assurer que le management du risque est efficace et contribue à l'atteinte des performances organisationnelles. Cependant, certains points particuliers à la surveillance et la revue du cadre de management du risque devraient être pris en compte :

- Mesurer les performances de management du risque par rapport à des indicateurs dont la pertinence est revue périodiquement ;

[1] ISO/IEC guide 73 ; op.cit ; p3.
[2] Pascal Kerebel; Management des risques, inclus secteurs banque et assurance; Collection Finance; Groupe Eyrolles; Éditions d'organisation; Saint-Germain; Paris; France; 2009; p61.
[3] ISO/IEC guide 73 ; op.cit ; p11.

- Mesurer périodiquement les progrès et les écarts par rapport au plan de management du risque ;

- Examiner périodiquement si le cadre organisationnel, la politique et le plan de management du risque sont toujours appropriés au vu du contexte interne et externe de l'entreprise, ainsi les outils et les procédures ;

- Établir des rapports sur les risques, sur les avancées du plan de management du risque, et sur la façon dont la politique de management du risque est suivie ;

- Vérifie l'efficacité du cadre organisationnel de management du risque, y compris les politiques applicables et les outils d'appui, en fonction du mandat et des principaux résultats et de l'évolution des principes et pratiques ;

- Produire des rapports sur le rendement et la valeur ajoutée de management du risque comme partie intégrante de la prise de décisions, de la planification des activités, de l'affectation des ressources et de management des activités compte tenu des contextes interne et externe ;

- Mener des analystes périodiques du contexte afin de relever de nouvelles approches, de nouveaux outils et de nouvelles idées ;

- Évaluer le retour sur l'investissement, tant qualitatif que quantitatif, des ressources, des outils et des activités destinés à la sensibilisation et à la formation des employés relativement aux questions liées au risque ainsi que d'autres résultats concrets de l'application systématique des pratiques de management du risque dans l'ensemble de l'organisation d'entreprise.

Dés lors, la documentation et la communication des activités de surveillance et de revue accroissent la capacité de l'entreprise à consigner ses résultats et à produire des rapports et améliorent son rendement en matière de management du risque. La préparation de rapports sur les résultats facilite l'apprentissage et améliore la prise de décisions, car les rapports servent à évaluer tant les réussites que les échecs et à diffuser des renseignements sur les pratiques exemplaires et les enseignements tirés.

Amélioration continue du cadre organisationnel « Continual improvement of the framework »

En plus de la surveillance et de revue, l'entreprise peut envisager d'autres activités qui lui permettraient d'améliorer son management du risque, tels que :

- Prendre en compte les commentaires, les observations et les recommandations élaborés suite à la surveillance et revue du cadre de management du risque ;

- Consulter les bonnes pratiques en matière de management du risque ;

- Remettre au diapason les approches de management du risque avec l'évolution des principes et des pratiques.

2. Gouvernance et responsabilités en matière d'Enterprise Risk Management

Le Corporate gouvernance d'entreprise, qui régit les relations entre le conseil d'administration, les organes de direction et les actionnaires peut être considéré comme une partie intégrante du dispositif d'Enterprise Risk Management.

En effet, une des caractéristiques de la manière dont le management du risque est intégré au sein de l'entreprise se reflète dans la compréhension, la définition et la détermination plus

ou moins claire des rôles et responsabilités ainsi la centralisation ou décentralisation de délégation des celles-ci.

Dans ce cadre, le directeur général en a la responsabilité ultime, les autres managers apportent leur soutien à la culture de l'entreprise en matière de management du risque, œuvrent en faveur du respect de son appétence pour le risque et gèrent les risques à l'intérieur de leur périmètre de responsabilités dans les limites de la tolérance au risque de l'entreprise. De même, le management du risque relève également de la responsabilité d'autres collaborateurs conformément aux directives et protocoles établis, dont la supervision est assurée par le conseil d'administration directement ou par ses comités.

Aussi, d'autres tiers, tels que les auditeurs externes, les autorités de tutelle, etc, sont également impliqués en fournissant les informations utiles au management du risque d'entreprise.

Nous répondons dans cette partie de notre recherche à la question : *Quelles sont les principaux contributeurs ou acteurs responsables en matière de management du risque au sein de l'entreprise?*

Cette question porte sur l'attribution de la responsabilité de management du risque et les acteurs qui assument cette responsabilité dans l'entreprise. Mais avant ça, nous devons éclairer les notions liés à la gouvernance d'entreprise en matière de management du risque, puis ses acteurs clés et l'interaction entre eux afin de s'assurer une bonne gouvernance du risque d'entreprise.

2.1. Préalable à Corporate gouvernance d'entreprise en matière d'ERM

Le terme de *Corporate gouvernance* peut être traduit sous deux expression, *le gouvernement d'entreprise* ou encore *la gouvernance d'entreprise*. Dont, il existe divers définitions à ce terme, nous avons choisi celles qui nous semblent appropriées à notre problématique de recherche.

Le comité Cadbury*, dans son rapport, définit la gouvernance d'entreprise par: « *The system by which companies are directed and controlled* », de même, par: « *the system or matrix of responsibilities of directors and shareholders by which companies are governed and controlled* [1]»

Toujours dans le même optique, l'Institute of Internal Auditors « IIA », traduit en français par Institut Français de l'Audit et du Contrôle Internes « IFACI », définit la gouvernance d'entreprise étant qu'un : « *Dispositif comprenant les processus et les structures mis en place par le Conseil afin d'informer, de diriger, de gérer et de piloté les activités de l'organisation en vue de réaliser ses objectif* [2]»

Encore, l'Organisation de Coopération et de Développement Économiques « OCDE » considère que : « *le gouvernement d'entreprise fait référence aux relations entre la direction d'une entreprise, son conseil d'administration, ses actionnaires et autres parties prenantes. Il*

* Définition du rapport Cadbury « Committee on the financial aspects of corporate governance » publiée le 1er décembre 1992.

[1] Jérôme Desponds; Gestion des risques et audit; Management et négoce internationaux; publié par ERNEST & YOUNG; HEG Genève; 2007; p16.

[2] Pierre Schick, Jacques Vera et Olivier Bourrouilh-Parège en collaboration avec AMF et IFACI; Audit interne et référentiels de risques : Gouvernance, Management des risques et Contrôle interne; Dunod; Paris; 2010; p7.

détermine également la structure par laquelle sont définis les objectifs d'une entreprise, ainsi que les moyens de les atteindre et d'assurer une surveillance des résultats obtenus[1] »

Dans ce cadre, Jacques Renard dans son ouvrage de références, distingue entre deux visions de gouvernance d'entreprise[2] :

➲ *La vision actionnariale de la gouvernance, ou Corporate gouvernance* : Elle privilégie les actionnaires et les dirigeants mandatés par eux. Dans ce contexte, une bonne gouvernance va s'attacher à l'information des dirigeants, aux structures et à l'éthique; la gouvernance va donc veiller à régler les conflits de pouvoir et conflits d'intérêts, de s'assurer que les organismes existantes permettent de superviser efficacement les dispositifs mis en place et qu'aucun d'entre eux n'est susceptible d'adopter un comportement déviant.

➲ *La vision partenariale de la gouvernance ou gouvernance opérationnelle* : Elle concerne l'ensemble des parties prenantes au sein de l'organisation, en prenant en compte le fonctionnement interne de l'entreprise, son management et son contrôle. Cette vision implique une attention toute particulière apportée aux ressources humaines, à la politique sociale, à l'information interne, à l'organisation opérationnelle, aux mécanismes de contrôles et de régulation.

Dans son livre blanc, l'IIA en a établi une liste des principaux éléments des bonnes pratiques en matière de la gouvernance d'entreprise, comme suit[3] :

- S'appuyer sur une organisation qui garantit un bon fonctionnement du conseil tel qu'un nombre de membres adéquats, existence d'autres comités émanant du conseil, procédures d'organisation des réunions, etc ;
- Prévoir que les membres du conseil possèdent les qualifications et l'expérience appropriées ainsi qu'une bonne connaissance du fonctionnement d'organisation ;
- Mettre à disposition du conseil, les ressources nécessaires pour des demandes de renseignements complémentaires afin d'en garantir l'interdépendance ;
- Contribuer à la définition de la stratégie de l'entreprise, notamment en dotent les acteurs de la gouvernance des informations nécessaires pour ce faire ;
- Contribuer à la définition de la structure organisationnelle qui participe à la réalisation de la stratégie de l'entreprise ;
- Instaurer une politique de gouvernance d'entreprise concernant la surveillance des résultats obtenus ;
- Prévoir les interactions nécessaires entre le conseil, la direction et les auditeurs internes et externes via un comité d'audit ;
- Contribuer à la mise en œuvre d'un système de contrôle interne efficace supervisé par la direction ;
- Définir les politiques et pratiques de rémunération, notamment celles concernant la direction générale, en accord avec les valeurs éthiques, les objectifs, la stratégie et l'environnement de contrôle d'entreprise ;

[1] Pierre Schick, Jacques Vera et Olivier Bourrouilh-Parège en collaboration avec AMF et IFACI; Audit interne et référentiels de risques : Gouvernance, Management des risques et Contrôle interne; Dunod; Paris; 2010; p7

[2] Jacques Renard; Théorie et pratiques de l'audit interne, Références; 7e Édition d'organisation; Groupe Eyrolles; Paris; 2010; p448.

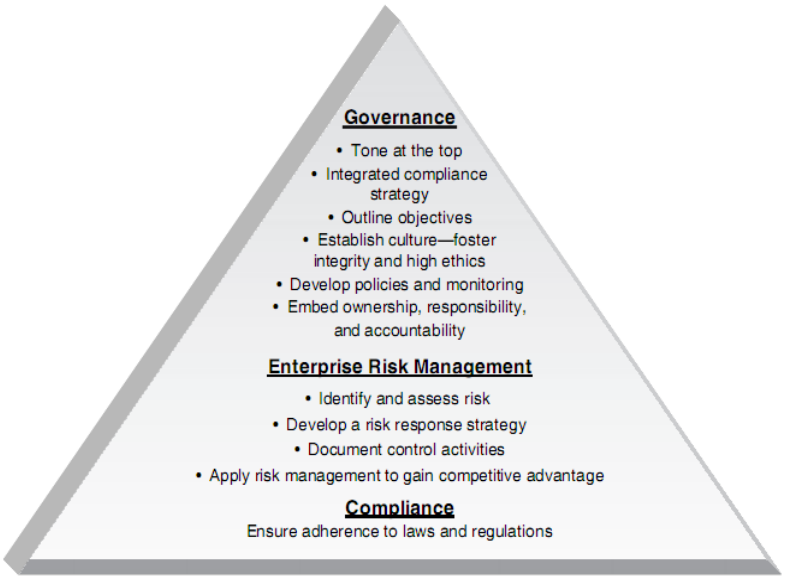
[3] P.Schick, J.Vera et O.Bourrouilh-Parège; op.cit; p8-9.

- Communiquer dans l'ensemble de l'entreprise une culture de la déontologie, les valeurs de l'organisation et la nécessité de l'exemplarité de la direction ;
- Faire appel de manière efficace aux auditeurs internes qui doivent disposer par ailleurs d'une indépendance pour garantir leur objectivité et de ressources suffisantes pour mener à bien leur mission ;
- Aussi, faire appel de manière efficace aux auditeurs externes en s'assurant de l'adéquation de leur indépendance, de leur ressources et de leur champ d'activité ;
- Définir et mettre en œuvre des politiques, processus et responsabilités en matière de management du risque au niveau de conseil et de l'ensemble de l'organisation ;
- Communiquer de manière appropriée les informations pertinentes aux parties prenantes ;
- Comparer les processus de gouvernance d'entreprise avec les bonnes pratiques reconnues et les réglementations en vigueurs.

Il est aisé de constaté, à la lumière de ce qui précède, l'implication de la gouvernance dans les fondements d'entreprise risk management. En effet, Anne M. Marchetti affirme que « *Corporate governance is a vital component of risk management. It provides the necessary top-down monitoring and management of risk associated with an organization. The topics of corporate governance and risk management are closely related, both focus on strategy and support of the strategic direction of the organization*[1] »

D'ailleurs, Anne M . Marchetti illustre cette relation transversale entre la gouvernance et le système d'Enterprise Risk Management sous la figure ci-dessous :

Figure N°11 : Enterprise Risk Management et la gouvernance d'entreprise



Source : Anne M . Marchetti ; op.cit ; p6.

Dans ce cadre de figure, E.Ebondo Wa Mandzila et D.Zéghal[2] soulignent que le management du risque et la gouvernance d'entreprise sont deux concepts indissociables.

[1] Anne M. Marchetti; Enterprise Risk Management Best Practices : From Assessment to Ongoing Compliance; Published by John Wiley & Sons, Inc Corporate; Hoboken; New Jersey; United States of America; 2012; p17.
[2] Eustache Ebondo Wa Mandzila et Daniel Zéghal; 2009; op.cit; p25.

Dont, l'enjeu pour la gouvernance est évidemment de se prémunir contre les risques internes et externes, opérationnels et stratégiques susceptibles de compromettre l'atteinte des objectifs tracés par l'entreprise.

De même, Mandzila considère que le contrôle et l'audit interne comme deux mécanismes de la gouvernance de l'entreprise, sensés réduire les risques auxquels l'entreprise est confrontée; ce qu'il est affirmé par le prolongement de COSO-I vers COSO-II, comme nous l'avons développé précédemment.

Encore sur la même vision, D.Zéghal et K.Lajili, présentent la relation entre le management du risque et la gouvernance d'entreprise sur deux volets[1] :

- La relation entre l'information et la surveillance, où les managers ont l'obligation de fournir une information à jour et pertinente au conseil d'administration et aux contrôleurs financiers sur les risques les plus importants auxquels l'entreprise est exposée et sur les l'efficacité des processus de management du risque adoptés une fois que les incertitudes sont révélées ;
- La deuxième relation concerne le lien entre l'information et l'incitation, où le conseil d'administration propose aux cadres dirigeants une rémunération visant à les inciter à gérer aux mieux des intérêts des actionnaires. Le niveau de la rémunération sera déterminé en fonction du risque encouru.

De ce fait, l'imposition d'exigences rigoureuses en matière de gouvernance d'entreprise est une condition préalable à l'efficacité de management du risque. In fin, pour mener bien le processus de management du risque, tous les organismes sont mises en avant, à charge pour toute l'entreprise de mettre en place ces fonctions pour améliorer la surveillance, le pilotage et la gestion de leur risques. Dont[2] :

- ***La surveillance des risques*** : Est l'ensemble des politiques et moyens mis en œuvre par l'organisation pour détecter, limiter et contrôler les risques liés à ses activités. Aussi bien, elle peut contribuer à l'identification et au management des opportunités en mettant en évidence les évènements et les facteurs tant internes qu'externes susceptibles d'avoir un impact favorable sur le développement de l'entreprise et la réalisation de sa stratégie.
- ***Le pilotage des risques*** : Le dispositif de pilotage des risques est mis en place par les dirigeants pour chaque entité de l'entreprise, qui définissent la politique de management du risque ainsi que la démarche et le dispositif de contrôle nécessaires à son application effective, il s'intégrant dans les modes de fonctionnement de l'entité, concourt à l'amélioration de sa performance et contribue à l'atteinte de ses objectifs. Ce dispositif s'appuie sur l'analyse et la synthèse des principaux risques à l'échelle de l'entreprise.
- ***La gestion des risques*** : Est la traduction opérationnelle du dispositif de pilotage des risques. C'est la mise en œuvre des processus d'identification, de hiérarchisation et de traitement des risques au niveau des activités par les responsables des directions, des grandes fonctions et de l'ensembles des collaborateurs. Dont, le management de chaque entité a la charge et veille à ce que l'exposition aux risques dans son périmètre d'activité soit conforme à la politique de management du risque définis par les dirigeants.

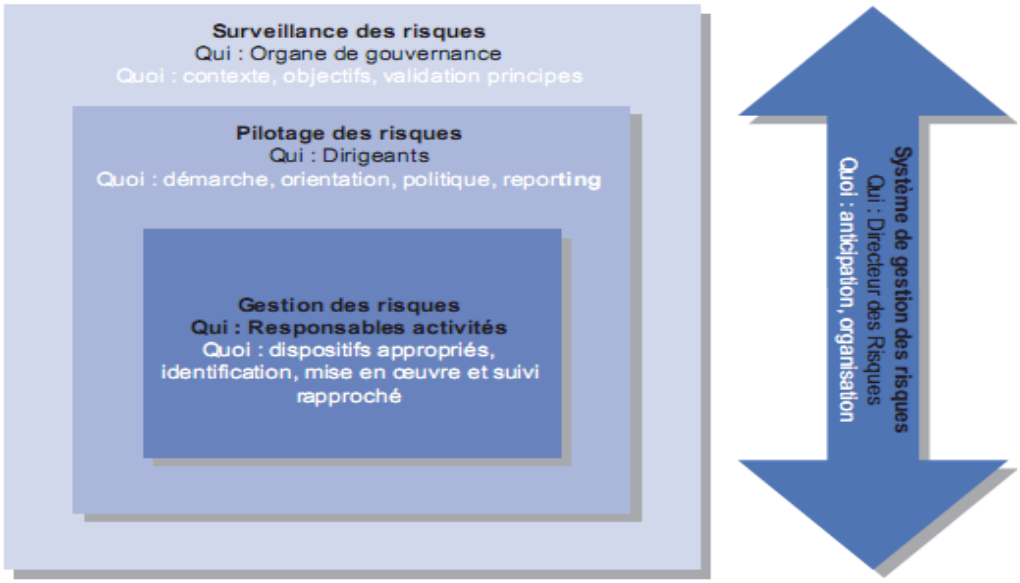
Alors, la vision globale du management du risque d'entreprise relève de la direction générale de l'entreprise qui délègue l'organisation des processus de management du risque à

[1] Lajili K et Daniel Zéghal; Gérer le risque à l'échelle de l'entreprise : L'autre facette de la gouvernance de l'entreprise; La Revue Gestion; Vol 30; Automne; 2005; p 106

[2] IFA, AMRAE en collaboration avec PwC et Landwell; Rôle de l'administrateur dans la maîtrise des risques; Paris; France; Juin 2009; p21-22.

une structure appropriée. Nous illustrons la relation entre surveillance, pilotage et gestion des risques comme suit :

Figure N°12 : Lien entre surveillance, pilotage et gestion des risques



Source : IFA, AMRAE en collaboration avec PwC et Landwell; op.cit; p22.

2.2. Rôles et responsabilités du conseil d'administration et ses comités dans l'ERM

La mise en œuvre et la supervision du dispositif de management du risque incombe à la haute direction, tandis que son pilotage est la responsabilité du conseil d'administration qui a pour rôle de guider la direction et d'apprécier la pertinence du dispositif de management du risque.

Aussi bien, le conseil d'administration prend connaissance de la stratégie et les risques auxquelles est exposée l'entreprise; il se préoccupe directement ou par ses comités de s'assurer si les actions mises en œuvre par le management permettront à l'entreprise d'atteindre ses objectifs et de maîtriser ses risques[1].

Conseil d'administration ou de surveillance

Sous le contrôle de l'assemblée générale, le conseil d'administration ou de surveillance, selon la forme juridique de l'organisation, détermine les orientations de l'activité de l'entreprise et veille à leur mise en œuvre. Il définit la stratégie de l'entreprise, fixe ses objectifs et ses attentes en termes d'intégrité et d'éthique, aussi, procède à l'affectation globale des ressources[2].

Le conseil d'administration supervise de management du risque au sein de l'entreprise et s'assure de l'efficacité des ses dispositifs. Il suit notamment l'efficacité des dispositifs de contrôle mis en place par le management pour garantir la qualité, fiabilité et conformité, des informations communiquées aux actionnaires et aux marchés[3].

[1] KPMG & FSIF; La gestion des risques et du contrôle interne au sein des sociétés foncières; publié par KPMG & Fédération des sociétés immobilières et foncières; Paris; décembre 2008; p38.
[2] IFACI, PwC et Landwell; COSO-II Report : Le management des risques d'entreprise-Cadre de référence et Techniques d'application; la traduction française par IFACI, PwC et Landwell en 2005; Troisième tirage 2007; Édition d'organisation; Groupe Eyrolles; Publication Février 2012; p 130.
[3] IFA, AMRAE en collaboration avec PwC et Landwell; Juin 2009; op.cit; p 25.

En effet, S.Cleary et T.Malleret[1] relèvent que le conseil d'administration doit déterminer la tolérance au risque de l'entreprise, la stratégie et la politique de risque en collaboration avec la direction exécutive et le top management, et veiller à ce que des processus adaptés, prenant en compte la compétence des employés, soient mis en place pour maîtriser et gérer les risques de manière proactive.

De plus, le conseil d'administration doit identifier les zones de risques clés et les indicateurs de la performance et les surveiller de manière à garantir que les systèmes de contrôle interne sont efficaces en fournissant aux actionnaires et autres parties prenantes une assurance raisonnable que les objectifs fixés seront atteints dans des conditions normaux ou difficiles, que ses actifs seront garantis, que toutes les lois ad hoc seront respectées, que les rapports seront précis et fiables et que l'entreprise se comportera de manière responsable à l'égard des parties prenantes.

S.Cleary et T.Malleret rajoutent que le conseil d'administration doit recevoir et examiner des rapports réguliers sur les processus de management du risque portant sur l'exposition de l'entreprise aux risques physiques et opérationnels, à ceux liés aux ressources humaines, aux risques technologiques, de crédit et de marché, de conformité ainsi aux provisions assurant la continuité d'exploitation et le recouvrement des pertes. De même, le conseil doit mettre en place des procédures de reporting confidentiel de type « Signal d'alarme » pour la fraude et les risques majeurs. Encore, le conseil s'assurer qu'une évaluation systémique et documentée des processus et des résultats portant sur les risques clés est effectuée au moins annuellement et que ses conclusions sont intégrées dans les rapports de conseil d'administration, où ce dernier doit affirmer sa responsabilité vis-à-vis du système de management du risque, préciser les processus de veille et de contrôle interne mis en place pour gérer les risques et maximiser les opportunités de l'entreprise, ainsi que les systèmes développés pour le management des crise.

Il convient au conseil d'administration de s'assurer que [2]:

- ✓ L'entreprise dispose d'une organisation, des moyens nécessaires et de procédures adaptées au management du risque ;
- ✓ Les administrateurs possèdent une connaissance pratique des activités de l'entreprise et de son environnement ;
- ✓ Le risque est pris en compte dans la réflexion et les décisions stratégiques ;
- ✓ L'information communiquée aux actionnaires leur donne une véritable compréhension sur les risques encours de l'entreprise.

Il est à noter, que le conseil d'administration peut choisir de déléguer ses responsabilités, sur certains points spécifiques, à un ou plusieurs comités ad-hoc; ces derniers n'agissent pas en vertu d'une délégation mais lui apportent assistance, leurs attributions en terme des propositions ou recommandations, sont définies dans une charte ou dans le règlement du conseil[3]. Aussi, en matière de management du risque, ces comités lui aideront à obtenir une vue claire en matière des risques d'entreprise.

Il est fréquent de trouver : un comité des nominations / de la gouvernance, un comité des rémunérations et un comité d'audit, les trois orientés sur des éléments distincts du dispositif de management du risque.

[1] Seàn Cleary et Thierry Malleret; Risques : Perception, Évaluation, Gestion; Une approche positive des risques globaux auxquels sont confrontés les décideurs; Édition Maxima; Paris; 2006; p72.
[2] KPMG & FSIF; Décembre 2008; op.cit; p 39.
[3] KPMG & FSIF; Décembre 2008; op.cit; p 40.

Le comité des nominations [1]

Le comité des nominations est en charge de l'identification et de l'examen des qualifications des administrateurs pressentis, il fait des propositions au conseil dans la sélection de nouveaux membres du conseil, le processus de succession des administrateurs et l'organisation de l'évaluation périodique du fonctionnement du conseil d'administration.

Notant que, l'IFA* recommande que tous les membres de ce comité soient indépendants.

Le comité des rémunérations [2]

Le comité des rémunérations considère de caractère adéquat du système et politique de rémunération des administrateurs, en s'assurant son cohérence avec les intérêts des actionnaires et la performance de l'entreprise. Il étudie en particulier les mécanismes d'intéressement et les programmes de motivation, par exemple : l'attribution gratuite d'actions, d'achat d'actions ou des bonus semestriels.

Le comité d'audit [3]

Le comité d'audit facilité la prise de décision du conseil d'administration, notamment dans trois domaines : les comptes et l'information financières, les risques et le contrôle interne et encore l'audit interne et externe. En effet, le comité d'audit constitue un pôle de compétences, auprès duquel le conseil d'administration peut demander assistance dans le management du risque.

Dans ce cadre, le rapport établi par KPMG & FSIF précise les principaux domaines d'intervention du comité d'audit comme suit :

✓ Le comité d'audit examine les comptes et vérifie la pertinence et la permanence des méthodes comptables adoptées dans l'élaboration des comptes consolidés de l'entreprise ;

✓ Il assiste le conseil d'administration dans sa mission de surveillance des risques et du contrôle interne de l'entreprise, particulièrement en :

- S'assurant de l'existence d'une procédure d'identification et de suivi des risques ;
- Examinant régulièrement une éventuelle cartographie des risques et des plans d'actions formulé ;
- Analysant la conformité aux obligations légales et réglementaires.

✓ Le comité vérifie les procédures internes de collecte et de contrôle des informations financières de l'entreprise ;

✓ Il formule une opinion sur l'organisation du service d'audit interne et examine son programme de travail ;

✓ En fin, le comité d'audit prend également connaissance des conclusions des auditeurs externes afin de rendre son avis au conseil d'administration.

On verra plus loin, dans le deuxième chapitre de cette thèse, plus amples de détail sur le rôle du comité d'audit dans le suivi de l'efficacité du dispositif de management du risque.

---

[1] KPMG & FSIF; Décembre 2008; op.cit; p 42.

* IFA : Institut Français des Administrateurs

[2] Idem; p 42.

[3] KPMG & FSIF; La gestion des risques et du contrôle interne au sein des sociétés foncières; publié par KPMG & Fédération des sociétés immobilières et foncières; Paris; Avril 2009; p 41.

En fait, l'IFA recommande que tous les membres des comités des rémunérations et de l'audit, soient indépendants et qu'au moins un des membres du conseil soit à la fois un membre de ces deux comités.

- ***Le comité des risques***[1]

Dans certaines entreprises, le conseil d'administration délègue la supervision de management du risque à d'autres organes que le comité d'audit car, le fait de demander au comité d'audit de superviser les risques non financiers, à savoir les risques opérationnels ou de conformité, cela dépasse l'objectif du ce comité et les ressources dont il dispose.

Dés lors, certains conseils d'administration ont mis en place un comité des risques pour s'intéresser directement au management du risque. Dans ce cas, les membres les plus expérimentés de la direction générale assistent aux réunions du comité.

Les responsabilités du comité des risques doivent refléter la collaboration de ce comité avec la direction générale sur les questions de développement et d'adaptation de l'appétence pour le risque et de tolérance au risque de l'entreprise.

À ce propos, le rapport COSO-II nous présente un modèle descriptif sur les périmètres d'activité du comité des risques en s'assurant l'efficacité du management du risque, illustrée ci-après :

[1] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 280.

Figure N°13 : Description du comité des risques

Objectifs du comité des risques

Le conseil d'administration, par l'intermédiaire du comité des risques, reconnaît qu'il est de sa responsabilité de s'assurer qu'un système de management du risque, incluant les politiques, les programmes, les mesures et les compétences pour l'identification, l'évaluation des risques significatifs, doit être en place pour assister la direction générale à gérer la croissance dans un environnement changeant rapidement

À cet égard, les objectifs spécifiques du comité des risques incluent le fait de s'assurer que :

- Le management comprend et accepte ses responsabilités en matière de management du risque ;
- La direction et le management des unités opérationnelles sont en ligne avec la stratégie de management du risque ;
- Les processus et les outils fournis aux différentes branches d'activité sont adéquats avec ses responsabilités en matière de management du risque ;
- L'évaluation des risques aux niveaux des unités opérationnelles est réalisée de façon permanente et exhaustive ;
- Les activités de traitement des risques liées aux unités opérationnelles permettent de :
  - Préserver les actifs ;
  - Maintenir des standards appropriés concernant l'environnement, la santé et la sécurité ;
  - Respecter les obligations légales et réglementaires ;
  - Renforcer les valeurs de l'entreprise en se concentrant sur les besoins des parties prenantes.
- Les registres comptables nécessaires sont tenus à jour, les politiques comptables adéquates ont été adoptées et les informations financières sont exhaustives et précises ;
- Le traitement des risques et les plans de test des contrôles sont en place et les résultats sont évalués et actés.

Les responsabilités du comité des risques

Ils incluent les éléments suivants :

- Superviser le développement et participer à l'analyse annuelle de la stratégie de management du risque d'entreprise ;
- Développer et adapter l'appétence pour le risque, ainsi la tolérance au risque de l'ensemble de l'entreprise ;
- Orienter et superviser le responsable des risques, tel que le Risk manager, ou les fonctions équivalentes ;
- Évaluer l'exposition de l'entreprise aux risques significatifs et en faire rapport au conseil ;
- Superviser les rôles et responsabilités de l'équipe de l'audit interne ;
- Revoir les comptes consolidés semestriels ou annuels.

Matérialité et orientation

Le comité des risques est chargé de s'assurer l'adéquation entre les compétences en matière de management du risque et la progression de l'appétence pour le risque de l'entreprise.

Le comité devrait revoir les risques qui pourraient s'avérer importants en accord avec les responsables des risques. Les considérations de matérialité seront basées à la fois sur l'exposition financières immédiate et à long terme des actionnaires.

Ce comité a le but d'encourager une réflexion plus large du management sur les risques et ce, afin qu'une attention plus grande soit portée à l'évolution des compétences de l'entreprise en fonction de leur vision de management du risque.

Réunions

Les réunions peuvent être trimestriels, semestriels ou annuels préalablement aux réunions de conseil d'administration.

Le directeur juridique, le responsable des risques ou le directeur du management du risque, le directeur financier ou d'autres peuvent assister à la réunion du comité des risques

En fin, un compte rendu de chaque réunion sera présenté au conseil d'administration.

Sources : IFACI, PwC et Landwell; COSO-II Report; op.cit; p 281-282.

En effet, le conseil d'administration a toute liberté de créer des comités qu'il juge opportun, dont on peut trouver dans certaines entreprises du comité de direction qualité et environnement ou encore appelé comité pour la qualité et le développement durable aussi, du comité d'investissement et d'arbitrage*, etc.

2.3. Rôles et responsabilités des acteurs du management en matière d'ERM

Le management est directement responsable de l'ensemble des activités de l'entreprise, y compris le dispositif de management du risque. Cette responsabilité varie selon les niveaux hiérarchiques et les caractéristiques de l'organisation.

Les enquêtes réalisées par le cabinet de conseil en matière de management du risque *Positiviti*[1], nous permettent de constater cette diversité en matière de responsabilité de management du risque, comme elles nous présentent le facteur évolutif de niveau de maturité de management du risque au sein des grandes entreprises.

Nous synthétisons les résultats de ces enquêtes depuis 2006 au 2011, sous le tableau ci après :

Tableau N°5 : La responsabilité des acteurs d'entreprise en matière de management du risque

	2011	2009	2008/7	2006
Direction Administrative et Financière	31%	21%	8%	3%
Président/DG/Comité de Direction	27%	53%	64%	56%
Direction des Risques	18%	8%	3%	7%
Direction de l'Audit Interne	10%	7%	5%	12%
Direction du Contrôle Interne	7%	1%	-	-
Responsables de Business Unit, de filiales ou d'usine	4%	3%	8%	5%
Direction de la Conformité	1%	5%	-	-
Comité des risques[2]	-	-	8%	17%
NSP/NR/Autre	2%	2%	4%	-

Source : Positiviti; Baromètre du Risk Management 2011 et 2009 ; Op.cit; P18.

On peut constater une évolution importante par rapport aux 2006 à 2009 avec la montée en puissance de la direction administrative et financière dans la responsabilité en matière de management du risque pour 31% des entreprises interrogées, alors que 27% d'entre elles, cette responsabilité incombe à la direction générale.

Ces résultats confirment que le management du risque impose l'attribution de responsabilités au niveau des différentes structures d'entreprise. La direction générale demeure ultimement responsable de ce dispositif dans son globalité, mais en organisant ses processus, la direction générale délègue des responsabilités à d'autres directions ou structures dont certaines sont plus spécifiquement consacrées au management du risque, telle que la

* Pour plus information vous pouvez consulter le rapport : KPMG & FSIF; décembre 2008.

[1] Positiviti; Baromètre du Risk Management 2011; Publication du Positiviti « Risk & Business Consulting, Internal Audit » en partenariat avec Tns sofres; 7ème Édition; 2011; p18-19.

[2] Positiviti; Baromètre du Risk Management 2009; Publication du Positiviti « Risk & Business Consulting, Internal Audit » en partenariat avec Tns sofres; 6ème Édition; 2009; p18.

direction des risques, d'audit interne et de contrôle interne, qui progressent de plus en plus par rapport aux années précédentes

La direction générale de l'entreprise

L'un des principaux aspects de ses responsabilités est de s'assurer de l'existence d'un environnement interne favorable. Elle doit s'assurer que tous les éléments du dispositif de management du risque sont en place.

La direction générale doit communiquer à tous les employés les valeurs éthiques et la philosophie de l'entreprise telles qu'elles sont déterminées par le conseil, instituer dans le langage et la culture de l'entreprise un système globale de management du risque intégré dans les activités quotidiennes des employés.

Pour ce faire, le directeur général remplir cette fonction[1] :

➲ En dirigeant et orientant les activités des managers; avec l'aide de autres membres de la direction, il établit les valeurs, les principes et les normes opérationnelles qui constituent les fondements du dispositif de management du risque au sein de l'entreprise ;

➲ En collaboration avec les directeurs, ils définissent la stratégie et les objectifs qui s'y rapportent, de même, ils élaborent les politiques globales et développent l'appétence pour le risque et la culture du risque de l'entreprise, ainsi que le type de système de reporting qui seront utilisés ;

➲ En se réunissant régulièrement avec les managers en charge des principales fonctions, commerciales, marketing, production, achats, finance, ressources humaines, etc, afin de passer en revue leurs responsabilités et particulièrement la façon dont ils abordent le management du risque. aussi bien, le directeur général s'informe des risques inhérents à l'activité, leurs traitements, les nécessaires améliorations des contrôles et de l'évolution de ceux-ci.

Cependant, certains directeurs généraux ont désigné un membre du management afin qu'il donne impulsion à la mise en place du dispositif de management du risque au sein de l'organisation, tandis que d'autres ont mis en place un comité pour cette fin. De même, une autre approche utilisée par un nombre croissant des entreprises, consiste à désigner un responsable des risques pour qu'il oriente, anime, donne des directives, soutienne et pilote les managers dans l'intégration et la mise en œuvre du dispositif de management du risque dans leur périmètre d'activité.

Comité exécutif de management du risque[2]

Lorsqu'il existe, ce comité rassemble des dirigeants expérimentés, de membres du management dont des managers fonctionnels comme le directeur financier, le directeur de l'audit, le directeur de la direction communication, etc.

Les responsabilités de ce comité sont illustrées ci-après sous sa charte, comme suit :

[1] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 132-133.
[2] Idem ; p 283.

Figure N°14 : La charte du comité du management du risque

Le comité de management du risque détermine les objectifs de l'organisation, son appétence pour le risque et ses seuils de tolérance aux risques. Il supervise le processus par lequel le management des unités opérationnelles identifie, évalue les risques et détermine les réponses appropriées.

Le comité définit les objectifs de mesures de performance et les indicateurs de risques clés. Il est responsable de la planification et de l'affectation des ressources, y compris celles allouées au management du risque, et des dépassements du budget.

Ce comité revoit également l'utilisation des ressources et la performance du management du risque par rapport au prévisionnel.

Source : IFACI, PwC et Landwell; COSO-II Report; op.cit; p 284.

La direction des risques et le Risk manager

Certaines entreprises de grande taille ou les plus complexes, ont mis en place un point de coordination centralisé afin d'améliorer et faciliter le management du risque, une direction des risques diriger par un responsable des risques encore appelé dans certaines entreprises « *Risk Manager* » ou « *Chief Risk Officer* », travaille avec les autres managers pour mettre en place un management du risque efficace au sein de l'ensemble de l'organisation. Le Risk manager est nommé par le directeur général et opérant sous la responsabilité direct de celui-ci.

La responsabilité de la direction des risques est de donner au directeur général une assurance raisonnable quant à la maîtrise globale des risques de l'entreprise, en mettant en place un dispositif structuré, permanent et adaptable permettant de s'assurer que les principaux risques sont bien identifiés, hiérarchisés, analysés et pondérés à leur juste valeur, et que l'organisation et les moyens mis en œuvre pour y répondre sont suffisants et adaptés.

En collaboration avec les directions opérationnelles et fonctionnelles, la direction des risques anime le processus global de management du risque. Elle établit la cartographie des risques ou la matrice des risques majeurs de l'ensemble de l'entreprise, synthétise les plans d'actions corrélatifs, mis en place de règles de conduite contribuant à un environnement interne cohérent et favorable à la maîtrise des risques, etc.

Nous reviendrons par la suite avec plus de détail sur la responsabilité, le rôle et la mission de risk manager.

Les directeurs et les managers en charge des unités opérationnelles[1]

Les divers responsables de branches d'activités, de processus opérationnels et de départements fonctionnels sont responsable sur leur périmètre de l'identification, de l'évaluation des risques, la mise en place des dispositifs de suivi et de vérification de leur bon fonctionnement. Ces responsabilité portant sur :

- La conformité aux politiques de management du risque et au développement des techniques adaptées aux activités de l'unité ;
- L'assurance que les risques sont correctement identifiés, évalués, pris en compte, communiqués et gérer au quotidien ;

[1] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 288.

- La communication au management des unités opérationnelles des rapports exhaustifs et complets sur la nature et l'étendue des risques liés aux activités.

L'audit interne

Les normes établies par l'Institut of Internal Auditors *« IIA »* précisent que l'audit interne a pour rôle d'évaluer l'efficacité du dispositif de management du risque, de contrôle et de gouvernance d'entreprise et de contribuer à leur amélioration continue sur la base d'une approche systémique et méthodique ainsi dans la formulation des recommandations[1].

Cette évaluation comprend la fiabilité de reporting, l'efficacité et l'efficience des opérations et la conformité aux lois, règlements et le respect des contrats. En cette qualité, l'auditeur interne peut soutenir la direction en lui fournissant une assurance sur[2] :

- Le processus de management du risque, à la fois leur conception et leur fonctionnement ;
- L'efficacité et l'efficience des traitements des risques et les activités de contrôles qui y sont associées, qui consistent à s'assurer que les principaux risques sont maintenus à un niveau acceptable ;
- L'exhaustivité et exactitude du reporting sur le management du risque, qui concerne la fiabilité et la qualité de l'évaluation et la bonne communication sur la maîtrise des risques d'entreprise.

Il est à noter que l'IIA précise que les entreprises doivent bien comprendre que la direction reste le responsable principal de management du risque; le rôle de l'auditeur interne consiste à donner des conseils et contester à soutenir les décisions de la direction concernant les risques, mais aucun cas l'auditeur interne ne prend ces décisions lui-même[3]. En effet, la nature des responsabilités et le rôle de l'auditeur interne doit être consignée dans la charte d'audit et avalisée par le comité d'audit.

On verra plus loin plus amples du détail sur la contribution et le rôle de l'audit interne dans le processus de management du risque de l'entreprise.

La direction ou la structure de contrôle interne [4]

Certaine entreprise ont dotées d'une direction du contrôle interne, structure ou département de contrôle interne en charge s'assurer la coordination des directions opérationnelles et fonctionnelles pour identifier, évaluer, normaliser et fiabiliser les processus clés de l'entreprise; favorisant l'amélioration des performances en mettant en place une organisation, des méthodes et des procédures pour chacune des activités de l'entreprise afin de garantir sa pérennité.

En effet, le contrôle interne dépend en amont d'un management efficace de tous les processus de l'entreprise, commerciaux, financières, techniques, ressources humaines, juridiques, etc. De même, le contrôle interne exige en aval un contrôle rigoureux de l'application des règles interne de l'entreprise, assuré par la direction de l'audit interne.

À ce titre, le rôle de contrôle interne s'articule autour de trois axes :

- Formaliser et mettre à jour les processus clés et les procédures largement diffusées et déclinées à l'échelle de l'entreprise ;

- Harmoniser les systèmes de management associés à leur mise en œuvre ;

[1] IFACI, PwC et Landwell; COSO-II Report; op.cit; p137
[2] Ibid ; p289.
[3] Institut of Internal Auditors; Le rôle de l'audit interne dans le management des risques de l'entreprise; L'IIA publications; Royaume-Uni et Irlande; Septembre 2004; www.iia.org.uk ; p2.
[4] IFA, AMRAE en collaboration avec PwC et Landwell; Juin 2009; op.cit; p 28.

- Veiller à l'adéquation des compétences avec les besoins de l'entreprise.

Le management des unités [1]

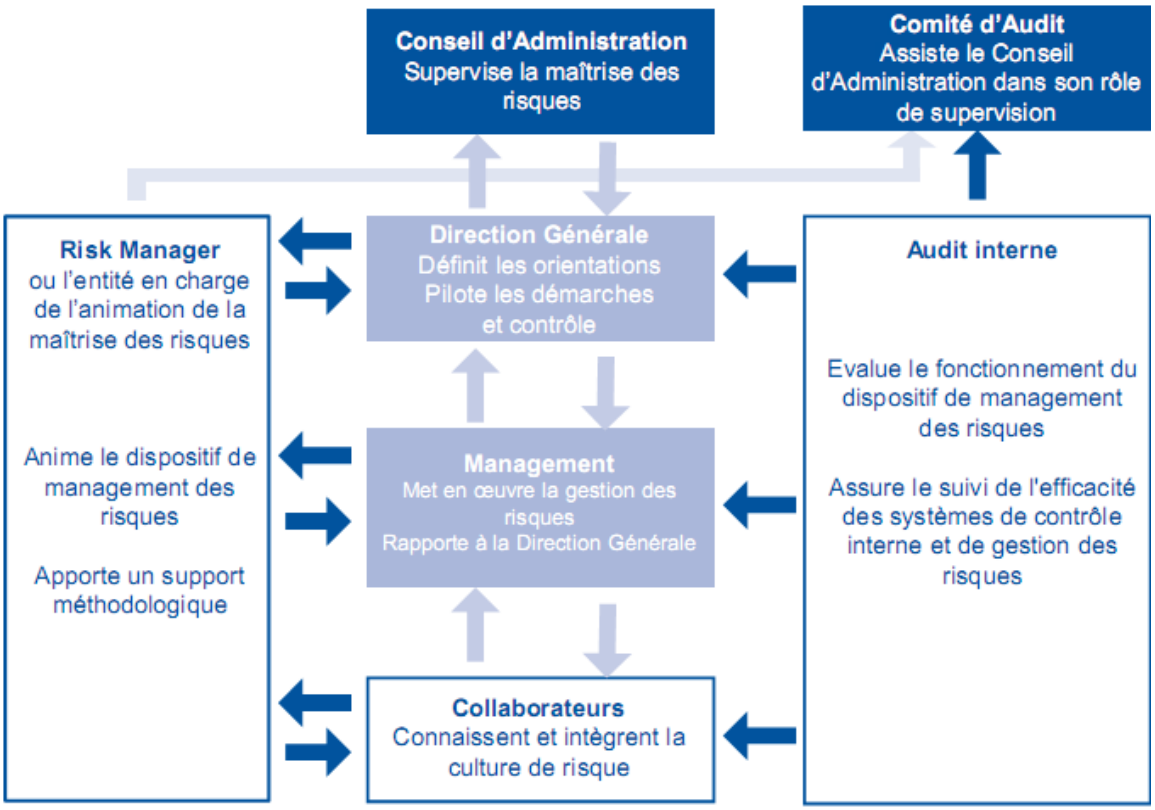
Le management ou le personnel de chaque unité opérationnelle ou fonctionnelle s'assure de l'application de la politique de l'entreprise en matière de management du risque lié à son périmètre d'activité.

Comme précède, la gestion des risques consiste la traduction opérationnelle du dispositif de pilotage des risques, c'est la mise en œuvre du dispositif d'identification, d'évaluation, traitement et communication des risques au niveau des activités par les responsables des directions et des grandes fonctions ainsi, par l'ensemble des collaborateurs.

Pour ce faire, chaque collaborateur doit avoir une connaissance de l'information nécessaires pour établir, faire fonctionner et surveiller les dispositifs de gestion des risques, au regard des objectifs qui lui ont été assignés.

Le schéma ci-dessous illustre le rôle des différents acteurs clés de l'entreprise dans un système globale de management du risque au sein de d'entreprise :

Figure N°15 : Les principaux contributeurs au management du risque d'entreprise



Source : IFA, AMRAE, PwC et Landwell; Juin 2009; op.cit; p 22.

En effet, le management du risque est l'affaire de tous et les rôles et responsabilités de tous les acteurs de l'entreprise doivent être clairement définis, soient être mentionnés de façon explicite ou implicite dans chaque description de ses postes.

[1] AMF; Les dispositifs de gestion des risques et de Contrôle Interne : Cadre de référence; Publication de l'autorité des Marchés Financiers; Juin 2010; p 13.

Les tiers

Il est probable que le management du risque proviendra de la contribution de différents acteurs, soient internes à l'échelle de l'entreprise, aussi bien externes, tels que les auditeurs externes, les experts, les législateurs et les régulateurs, les commissaires aux comptes et même les fournisseurs et les clients de l'entreprise, etc. Ces acteurs peuvent fournir des informations utiles à l'entreprise quant à son dispositif de management du risque.

Les auditeurs externes [1]

L'auditeur externe fournit au management du risque et au conseil d'administration un point de vue unique, indépendant et objectif sur la régularité et la sincérité des comptes comptables, conformément à la loi en vigueur, qui peut contribuer, entre autre, à la réalisation des objectifs de l'entreprise en matière de communication financière externe; ainsi l'auditeur externe apporte au management du risque des informations utiles, incluent :

- Les conclusions de la mission d'auditeur externe, des informations analytiques et des recommandations ;
- Les conclusions sur les défaillances du dispositif de management des risques et les contrôles révélés à l'auditeur au cours de sa mission, et ses recommandations pour y remédier.

Les commissaires aux comptes [2]

Les commissaires aux comptes ne sont pas, dans le cadre de leur mission légal, partie prenante de dispositif de management du risque de l'entreprise. Ils en prennent connaissance, s'appuient sur les rapports de l'audit interne lorsqu'il existe, pour avoir une meilleure appréhension et se font en toute indépendance une opinion sur leur pertinence.

En certifiant les comptes, le commissaire aux comptes peut identifier au cours de l'exercice des risques significatifs et des faiblesses majeures de management du risque et de contrôle interne, susceptibles d'avoir une incidence significative sur les informations comptables et financières.

Le commissaire aux comptes présente ses observations sur le rapport du président, pour celles des procédures de contrôle interne qui sont relatives à l'élaboration et au traitement des informations comptables et financières, et atteste l'établissement des autres informations requises par la loi en vigueur.

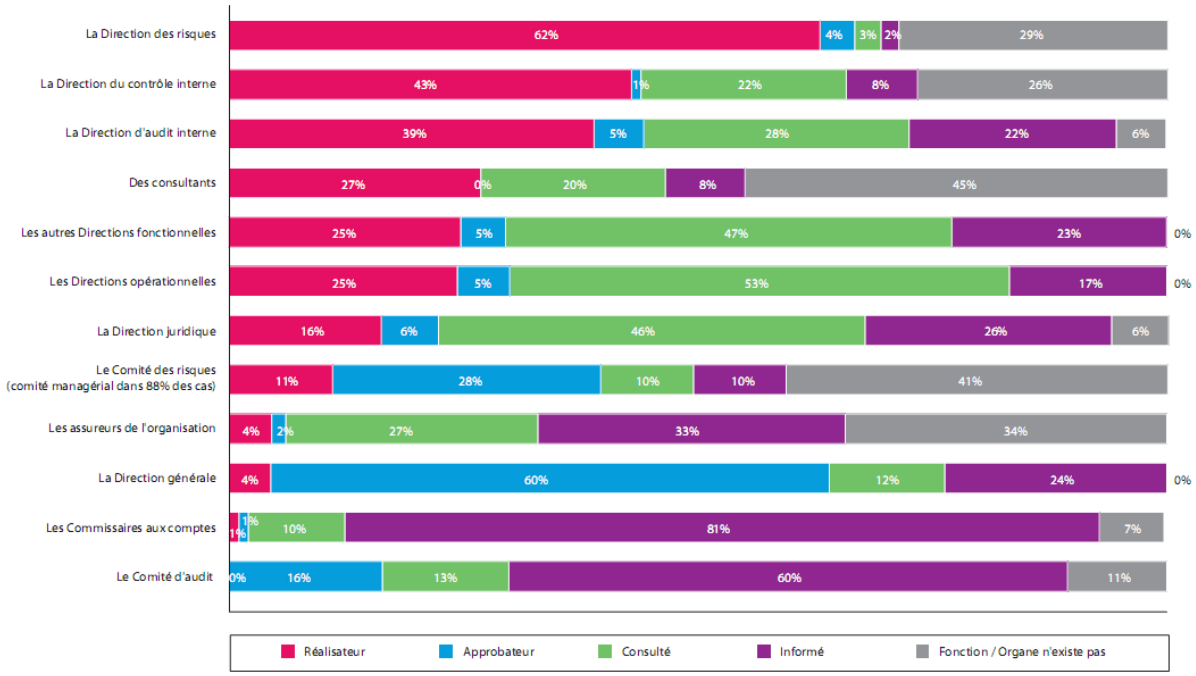
Les législateurs et régulateurs [3]

Les législateurs et les régulateurs ont double influence sur le dispositif de management du risque de l'entreprise; d'un coté, les obligations à mettre en place des mécanismes de management du risque et de contrôle interne, ce qui oblige l'entreprise à s'assurer que son système de management du risque répond aux exigences statutaires et légales en vigueur. De même, ils fournissent des recommandations, des lignes directives aidant les entreprises à améliorer ses dispositifs de management du risque.

[1] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 140.
[2] AMF; Les dispositifs de gestion des risques et de Contrôle Interne : Cadre de référence; Juin 2010; Idem ; p13.
[3] IFACI, PwC et Landwell; COSO-II Report; op.cit; p 141.

Pour conclure, nous s'avère utile de présenter les résultats de l'enquête réalisée par IFACI[1] auprès 724 entreprises, sur la problématique du rôle des parties prenantes dans l'évaluation formelle des risques.

Figure N°16 : Rôle des parties prenantes dans l'évaluation formelle des risques



Source : IFACI, Les pratiques de l'audit et du contrôle internes en France en 2009; JANVIER 2010; p 25.

Selon cette enquête, il ressort que la nécessité de clarifier les responsabilités s'impose encore plus lorsqu'on analyse l'implication des autres parties prenantes de l'évaluation formelle des risques. Les principaux réalisateurs de l'évaluation sont la direction des risques (62%), la direction du contrôle interne (43%) et la direction de l'audit interne (39%). Celle-ci a un spectre de responsabilité beaucoup plus large parce qu'elle est également consultée (28%) ou informée (22%).

Les autres opérationnels et autres directions fonctionnelles sont surtout consultés (environ 50% des cas) mais ils réalisent également cette évaluation des risques dans ¼ des cas.
Les organes de gouvernance ont des rôles bien distincts et complémentaires. Le comité d'audit n'est jamais réalisateur de l'évaluation. Il est surtout informé (60%). L'approbation de l'évaluation des risques est essentiellement du ressort de la direction générale (60% des cas). Ces deux instances sont consultées dans les mêmes proportions. L'implication du comité des risques est plus grande que celle du comité d'audit. Il est vrai que le comité des risques a un mandat plus spécifique en la matière. Il est souvent exclusivement composé de managers (dans 88% des cas) ce qui explique le rôle de cette instance en matière d'approbation de l'évaluation des risques (29%) et de réalisation de l'évaluation (11%).

Et enfin, Les commissaires aux comptes sont surtout informés (80%). Ils sont consultés dans 10% des cas.

[1] IFACI, Les pratiques de l'audit et du contrôle internes en France en 2009; institut français de l'audit et du contrôle interne; en partenariat avec ESSEC (business school paris-singapore); paris; janvier 2010 p 25.

3. La fonction de Risk Management

Le risk manager a une fonction transverse dans l'entreprise ayant à intervenir sur des enjeux extrêmement variés, il n'existe pas de référentiel de la fonction de risk-manager. Il existe seulement une fiche emploi/métier du Répertoire National des Métiers et des Emplois (ROME), très sommaire, et une liste de tâches assumées par le risk-manager, déposées sur le site de l'AMRAE (www.amrae.fr) ou décrites par Veret et Mekouar (2005). La fonction de risk-manager recouvre donc des acceptions différentes qui concernent souvent un seul aspect ou un domaine d'action de la gestion des risques. Elle est par ailleurs très hétérogène selon les entreprises.

Le rôle du Risk Manager continue d'évoluer et de se renforcer par rapport à son périmètre d'activités, dans son rattachement et dans son implication dans la stratégie de l'entreprise.

3.1. Définition et focus sur la fonction de Risk Manager

La notion « *risk manager* » est floue, elle peut considérée comme relevant du risk manager « *toute action qui s'appuie sur une méthodologie intégrant l'analyse, la réduction et/ou le transfère de risque ainsi le retour d'expérience*[1] »

Le risk manager est traduit en français par « *le gestionnaire de risque* » est celui qui conduit les actions de gestion des risques, dont cette dernière est la traduction opérationnelle du dispositif de management du risque par les responsables des directions, des grands fonctions et l'ensemble des collaborateurs. Or le risk manager tel que l'entendent les Anglo-Saxons n'est pas un simple gestionnaire mais un « *visionnaire* » de risques capable d'avoir une approche globale des risques encourus par l'entreprise. Cette traduction en français lui fait donc partiellement perdre de sa spécificité. De plus, dans l'esprit de nombreux praticiens, le terme de gestionnaire des risques est trop marqué par ses origines dans le monde de l'assurance[2]. Ces éléments nous amènent à préférer parler de risk manager.

Le terme Risk-manager est retenu par l'Association pour le Management des Risques et des Assurances de l'Entreprise « AMRAE », déterminant dans son rapport « Le Baromètre de Risk Manager », édition 2011[3], une liste des titres de cette fonction qui peuvent correspondre aux trois catégories principales des activités :

Figure N°17 : Focus sur les titres de Risk Manager

AP	AP & ERM	ERM
Directeur Assurances et Prévention	Directeur Management des Risques et des Assurances	Directeur Gestion des Risques
Directeur des Assurances	Directeur Gestion des Risques et des Assurances	Directeur Management des Risques
Group Insurance Manager		Chief Risk Officer
Group Insurance Engineer		Risk Officer
Group Risk Manager		
Risk Manager		
Directeur des Risques et Assurances		
Risk & Insurance Manager		

Source : AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p7.

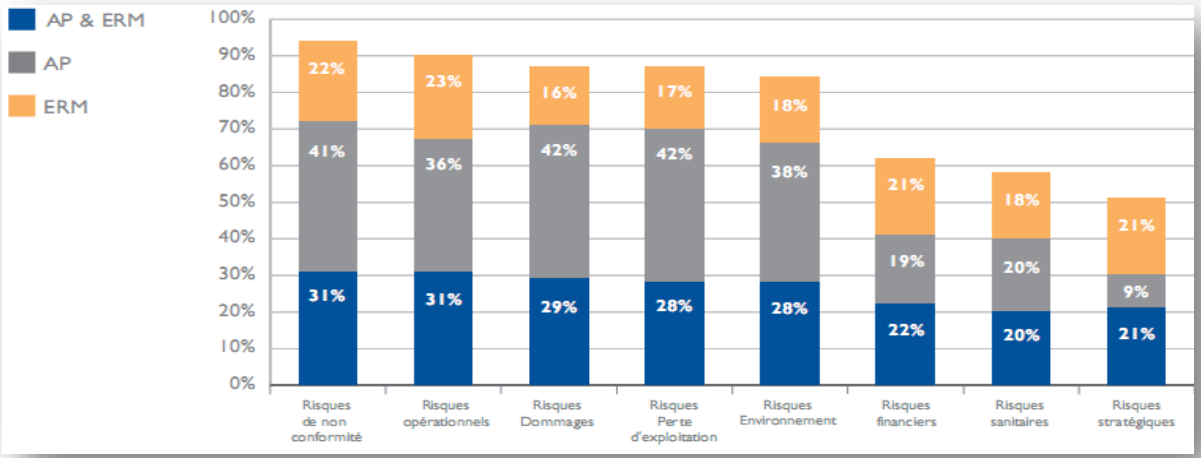
[1] Catherine Véret et Richard Mekouar ; op.cit ; p47.
[2] Caroline Aubry & Marie-Annick Montalan; Comment définir la fonction de Risk-Manager? Proposition d'un projet d'étude terrain des pratiques managériales en matière de risques opérationnels (à l'environnement, aux personnes, aux biens...); revue Comptabilité et environnement; France; 2007; p6.
[3] AMRAE ; Le Baromètre de Risk Manager; Publication AMRAE en partenariat avec Deloitte; Paris; France; Edition 2011; www.amrae.fr ; p7.

En fait, le titre de cette fonction peut traduire un tel niveau de maturité de l'organisation de risk management au sein de l'entreprise. Dont, les résultats du baromètre Risk Manager 2011, nous montre que parmi les 106 Risk manager ayant participés à l'enquête, on peut distinguer les trois catégories d'activités figurées ci-avant comme suit[1] :

- ***L'Assurance et la prévention « AP »,*** présente 45% de activité des répondants ;
- ***L'Entreprise Risk Management « ERM »*** y compris le contrôle interne, présente 24% de l'activité des répondants ;
- En fin, les activités à la fois orientées vers l'assurance et la prévention et vers le management globale du risque ***« AP & ERM »***, présente 31% de l'activité des risk manager participants.

À cet égard, l'enquête AMRAE (2011) ressort une variété d'univers des risques gérés par le risk manager comme s'affichant les résultats ci-dessous :

Figure N°18 : L'univers des risques gérés par le Risk Manager



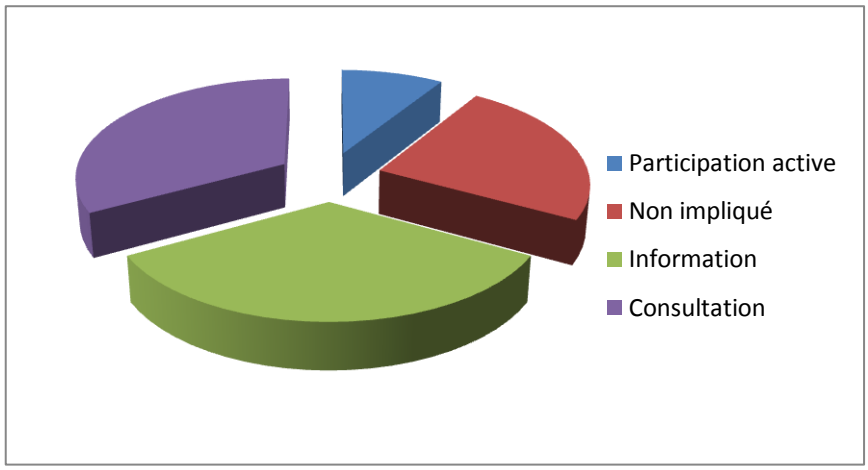
Source : AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p10.

En raison de son caractère transversal de la fonction de risk manager, ce dernier peut gérer une palette variée des risques, allant des risques opérationnels, de non-conformité, des risques financiers aux risques stratégiques.

De même, le risk manager peut dés lors contribuer au processus décisionnel en apportant son regard objectif sur la prise des risques et la capacité de l'entreprise à les maîtriser. Cette implication de risk manager dans la stratégie variée selon la culture et la politique et l'organisation de l'entreprise.

[1] AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p6.

Figure N°19: L'implication de Risk Manager dans la stratégie de l'entreprise



Source: AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p10.

L'enquête AMRAE (2011) conclu que 42% parmi les 106 risk manager interrogés sont concernés par la stratégie de l'entreprise, 9% présentent une participation active, 33% sont consultés, alors que 34% sont informés, voire non impliqués 24%[1].

3.2. L'organisation de la fonction Risk Manager

Certes, le Risk manager, c'est avant tout un état d'esprit mais concrètement implanter cette fonction et crées tout un département ou un poste risk manager, revient à traiter de multiples questions, avec des enjeux de pouvoir quelquefois complexes.

- Est-ce une fonction stratégique ou un poste pérenne ? est-ce un projet ou un processus support ?
- Comment et par qui cette fonction est-elle en charge ?
- À qui doit-on rattacher la fonction ?
- La fonction doit-elle être centralisée ou non ?
- Toutes les activités sont-elles concernées ?
- …etc

La réponse à ces questions n'est pas aussi simple et dépend avant tout du contexte et de particularité de l'entreprise ; nous essayons ci-après de tracer les grandes lignes de la fonction Risk manager en les confronter avec quelques bonnes pratiques tirées des enquêtes internationaux liées à notre problématique.

➲ *Rattachement de la fonction Risk Manager*

Le niveau de rattachement de la fonction risk manager dans l'organisation est un indicateur représentatif du niveau de maturité de l'entreprise face au risque ; Selon l'enquête réalisée par AMRAE en 2011, parmi les 106 risk manager interrogés, 17% se trouve au niveau « N-1 » de la direction générale DG ou au CEO « *Chief Executif Officer* », soit 47% au niveau « N-2 » de ces derniers.

La littérature et les enquêtes sur ce sujet révèlent qu'au niveau fonctionnel, le risk manager est rattaché soit au niveau de décision, soit à celui des opérations. Or, hiérarchiquement parlant, la fonction de risk manager est par nature transverse, indépendante, et par voie de

[1] AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p10.

conséquence en ligne directe avec la direction générale DG et/ou direction financière, 18% et 30% respectivement selon les résultats de l'enquête « AMRAE 2011 ».

Notant que ce rattachement directe de la fonction de risk manager au DG/CEO est particulièrement fréquent lorsque la fonction à été récemment créée, soit 88% pour les risk manager type « ERM », 71% pour celui de « ERM & AP » et enfin 33% pour le type de « AP » [1].

On peut encore observer des rattachements au comité exécutif, au secrétariat générale (17%, AMRAE 2011), à la direction juridique (18%, AMRAE 2011), les directions opérationnelles, l'audit interne voire même à la direction de l'organisation, de logistique et à la direction des achats[2].

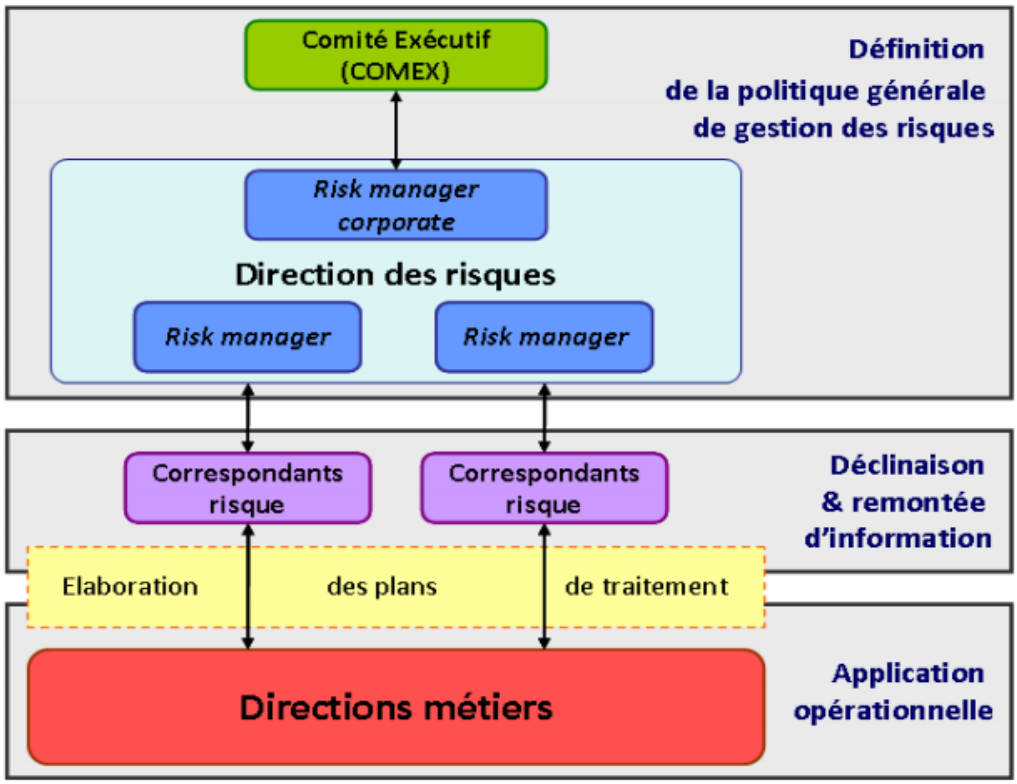
➲ ***Les organigrammes possibles en matière d'entreprise risk management***

Lors des entretiens réalisés par J.Lacroix[3] , on peut en effet distinguer quatre modes principaux d'organisation de la fonction de Risk manager mise en place dans les entreprises.

✓ *Organisation globale d'Entreprise Risk Management*

L'organisation globale en matière de risk management est liée à l'adoption d'une politique globale et intégrée de management du risque au sein de l'entreprise, cette politique favorise l'utilisation des méthodologies et d'outils communs à l'ensemble des directions, structures ou filiales de l'entreprise afin de structurer et de rendre cohérente l'implication de ces entités à la démarche de Risk Management ; dont, elle permet d'avoir une vision complète sur risques encourus de l'entreprise, principalement les grandes entreprises ou les groupes décentralisés.

Figure N°20 : L'organisation globale d'Entreprise Risk Management



Source : Jérémie Lacroix; CIGREF & IERSE; 2007; op.cit ; p20.

[1] AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p11.
[2] Catherine Véret et Richard Mekouar ; op.cit; p68.
[3] Jérémie Lacroix; CIGREF & IERSE; 2007; op.cit ; p20.

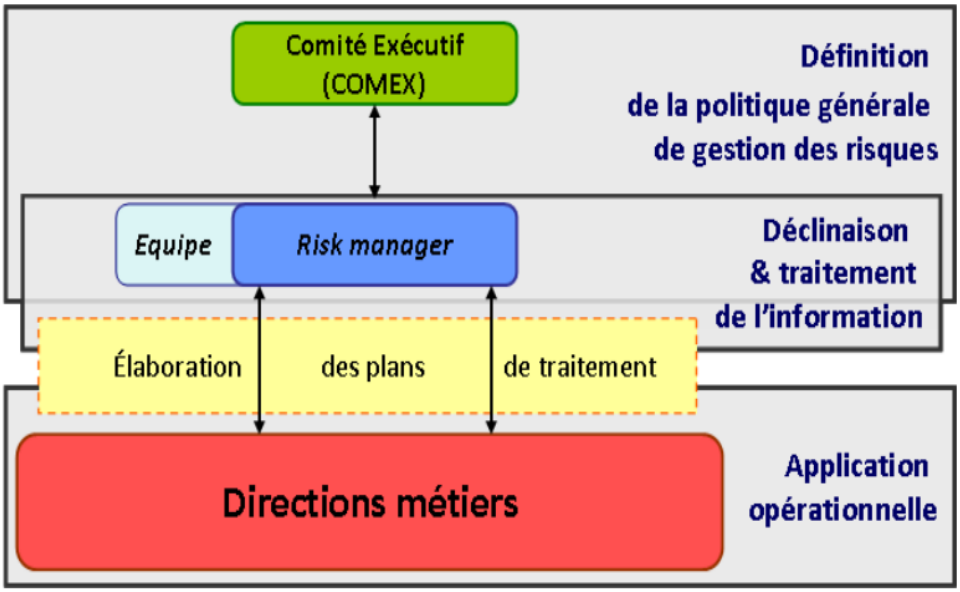
En fait, la mise en œuvre de cette politique globale est sous la responsabilité d'un risk manager le plus souvent rattaché au comité exécutif qui définit avec son aide, les éléments de cette politique générale de risk management. Le *risk manager corporate* ou *CRO* « *Chief Risk Officer* »a un rôle de coordinateur et de superviseur de la démarche et par conséquence, il va dans certains cas avoir la responsabilité de la direction de l'assurance ou du contrôle interne.

Dans ce cas, le directeur des risques est assisté par des correspondants participent à la remonté des informations nécessaires à la cartographie des risques de l'entreprise. Dont, les directions métiers sont compétentes pour l'application opérationnelle de la politique de risk management dans leur périmètre d'activités.

✓ *Organisation centrale réduite d'Entreprise Risk Management*[1]

Les entreprises fortement centralisées ou mono-sites adoptent plus généralement ce mode d'organisation en matière de risk management. En effet, assisté d'une petite équipe, le risk manager d'entreprise ou *CRO* définit la politique générale de management du risque.

Figure N°21 : L'organisation centrale réduite d'Entreprise Risk Management



Source : Jérémie Lacroix; CIGREF & IERSE; 2007; op.cit ; p22.

Le risk manager a pour interlocuteurs directs, les directions métiers et les opérationnels avec lesquels il établit la cartographie des risques, aussi bien les plans d'action nécessaire à leur traitement.

Dans ce mode d'organisation, il n'y a pas de correspondants risques ou équivalents dans les filiales et dans les différents divisions de l'entreprise ou du groupe.

✓ *Organisation en électron libre d'Entreprise Risk Management*[2]

Certes que l'absence de risk manager dans une organisation ne signifie pas l'absence d'une démarche de management du risque. En effet, la mise en œuvre d'une telle démarche peut être initiée par une direction métier ou une direction fonctionnelle qui donne les impulsions nécessaires à cette démarche.

[1] Jérémie Lacroix; CIGREF & IERSE; 2007; op.cit ; p21.
[2] Jérémie Lacroix; CIGREF & IERSE; 2007; op.cit; p22.

Ce mode d'organisation peut dans certains cas provoquer un manque de visibilité de la démarche, relayée par l'absence d'une politique globale et intégrée de risk management et encore elle peut aussi conduire à moins d'efficacité et de cohérence dans la mise en œuvre de la démarche de management du risque.

✓ *Absence d'organisation ou organisation intuitif d'Entreprise Risk Management*[1]

Ce mode d'organisation prédomine dans les entreprises caractérisées par une gestion traditionnelle des risques, lorsqu'il n'existe ni risk manager ni démarche structurée de risk management. Dont, les différentes structures assurent indépendamment au niveau local l'identification et le traitement de leurs propres risques.

Cette conception indépendante ne permet pas un management centralisé des risques, ni d'une coordination entre les programmes de contrôles et de maîtrise des risques.

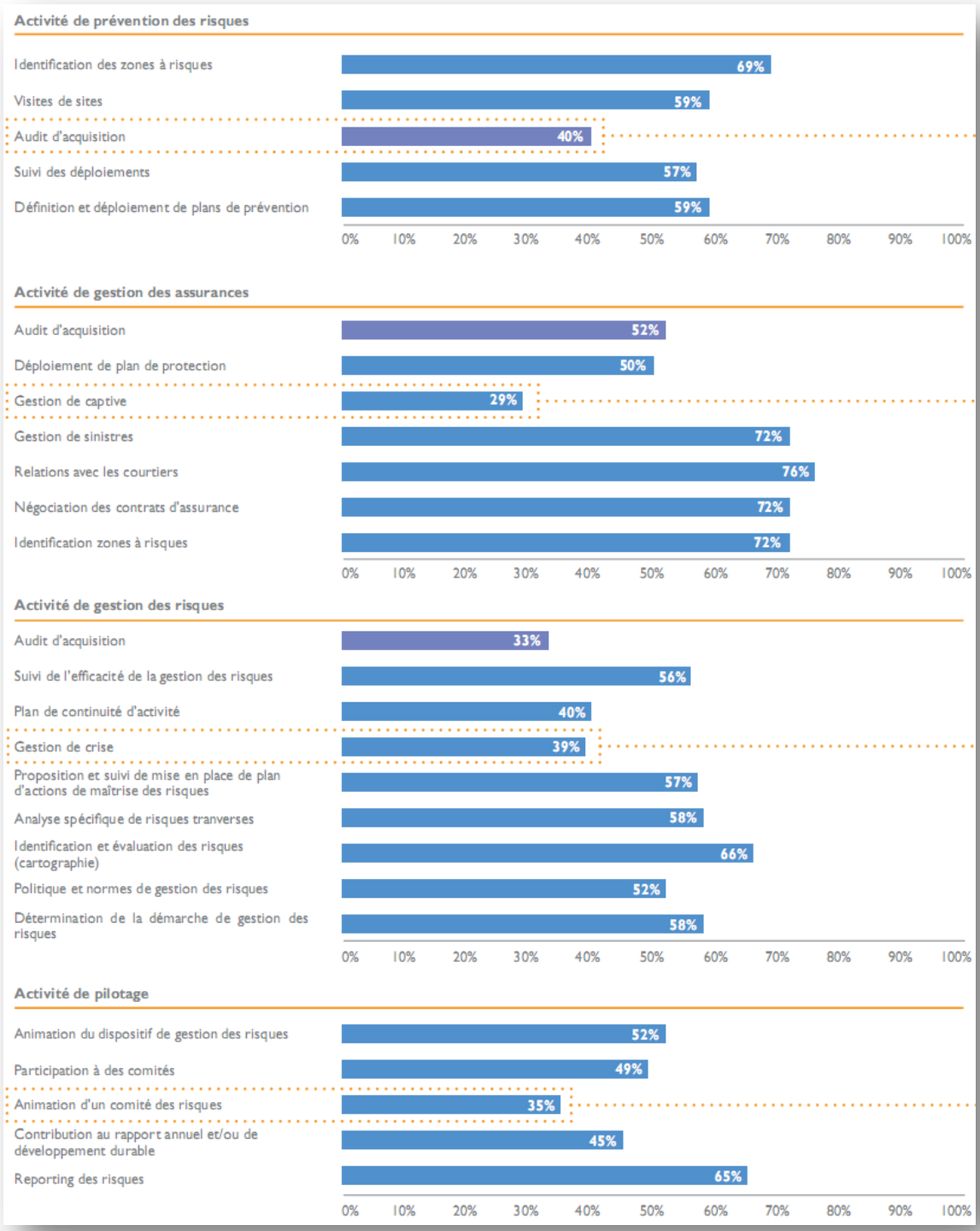
3.3. Description de fiche de poste du Risk manager

Toujours dans la même vision de clarifier les principales composantes caractérisant la fonction de Risk management au sein de l'entreprise, et en vue d'aborder le périmètre de cette fonction incluant les rôles, les responsabilités, les missions, les taches ainsi les critères indicatifs de performance et le profil de risk manager ; nous proposons ci-après les grandes lignes descriptives du fiche de poste de responsable de Risk management comme suit :

- ***Rattachement fonctionnel et hiérarchique***, déjà traité précédemment ;
- ***Périmètre d'intervention du risk manager*** : la figure ci-dessous illustre les principaux domaines d'intervention des risk managers liés aux activités de prévention, activités d'assurance, les activités de management du risque et enfin, les activités de pilotage :

[1] Jacques Charbonnier; Le risk management : Méthodologie et pratiques; Éditions L'Argus de l'assurance; Paris; France; 2007; p247

Figure N°22 : Le périmètre d'intervention du Risk Manager



Source : AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p8.

Il ressort que le risk manager englobe surtout les activités d'assurance, soit 72% parmi des interrogés prennent en charge la responsabilité d'identification des zones à risques ainsi la négociation des contrats d'assurance. Tandis que certaines entreprise telles que France Télécom confient à leur risk managers une véritable fonction de management du risques basée sur une démarche globale structurée. Dont, l'élaboration de la cartographie des risques s'affirme comme une priorité pour 66% des entreprises.

Il semble toutefois que le plan de continuité d'activité et le management de crise se trouvent parmi les missions et les activités de ce manager pour 40% et 39% respectivement des entreprises. Cependant, le système d'information et de reporting des risques arrive en tête avec 65% des réponses sur les activités du pilotage du risk manager puis l'animation du dispositif de risk management par 52% des réponses.

✍ ***Rôles, responsabilités***, consistent à [1]:

- Agir en tant qu'accompagnateur de la direction en l'aidant à concevoir et à mettre en œuvre une architecture de management du risque adaptée et approprié à l'entreprise ;

- Surveiller le profil de risque à l'échelle de l'entreprise et d'assurer que les risques significatifs sont identifiés et qu'ils font l'objet d'un rapport ascendant ;

- S'assurer de l'appropriation adéquate de management du risque pas les responsables opérationnels et une supervision efficace par les équipes de la direction des risques conformément à la politique et la structure de management du risque ;

- Promouvoir une compétence en matière de management du risque au sein de l'entité en développant un savoir faire et une expertise et en aidant les managers opérationnels à mettre en adéquation les traitements des risques avec la tolérance au risque, ainsi qu'en définissant les contrôles appropriés ;

- Élaborer un langage commun en matière de management du risque ;

- Faciliter le développement par les managers de protocoles de reporting qui tiennent compte de seuils quantitatifs et qualitatifs et superviser le processus de reporting ;

- Rendre compte à la direction générale des progrès et améliorations et recommander des actions nécessaires ;

- Assister les auditeurs internes et externes à se baser sur les rapports de management du risque d'entreprise pour des besoins de planification et de réalisation des missions d'audit ;

- Assister le conseil d'administration dans l'accomplissement de ses responsabilités en matière de gouvernement d'entreprise ;

- Faciliter, remettre en question, accompagner et orienter l'approche intégrée de management du risque d'entreprise ;

À ce titre, IFA et AMRAE nous proposent une feuille de route liée au périmètre d'activité de la direction ou département de management du risque, inclut[2] :

- ***Connaître et anticiper*** : s'assurer une veille permanente sur les risques ;

- ***Organiser*** : s'assurer la prise en compte des risques significatifs au niveau approprié ;

- ***Contrôler*** : s'assurer la mise en place adéquat des moyens et d'organisation ;

- ***Informer ou reporter*** : s'assurer une bonne communication sur la performance du dispositif de management du risque à l'égard des parties prenantes et au marché d'entreprise.

✍ **Principaux interlocuteurs** : incluant

- Les actionnaires ;
- Les dirigeants de l'entreprise ;
- Les personnels de l'entreprise ;

[1] Institut of Internal Auditors; Aller de l'avant avec la gestion du risque d'entreprise; IIA publications; Juin 2007; p3.
[2] IFA, AMRAE en collaboration avec PwC et Landwell; Juin 2009; op.cit; p 28.

- Les fournisseurs ;
- Les clients ;
- Les partenaires économiques ;
- Le législateur et les autorités de tutelle, etc.

Critères indicatifs de performance

Selon les risk managers interrogés par l'enquête de l'AMRAE en 2011, les principaux critères qualitatifs et quantitatifs ayant un impact sur le rendement et la performance du Risk manager peuvent être groupés sous les trois catégories d'activités, qu'on a déjà mentionné précédemment, comme suit :

- Risk manager catégorie « Assurance, Prévention et Enterprise Risk Management, *AP & ERM* », les critères les plus cités sont :

Tableau N°6 : Les critères qualitatifs et quantitatifs de la performance du Risk Manager catégorie « AP & ERM »

	AP & ERM	
	Critères quantitatifs	Critères qualitatifs
1	Résultats	Objectifs
2	Objectifs (groupe/individuels)	Diffusion de la culture risque du groupe
3	Coûts	Déploiement du projet
4	Baisse des sinistres	Capacité de travailler en transverse
5	Renouvellement des contrats	Relationnel

AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p23.

- Risk manager catégorie « Enterprise Risk Management, *ERM* », les qualités incluent :

Tableau N°7 : Les qualités techniques et personnelles du Risk Manager catégorie « ERM »

	ERM	
	Qualités techniques	Qualités personnelles
1	Performance collective	Qualité du reporting et respect des échéances
2	Déploiement de la cartographie des risques	Transversalité
3	Objectifs groupe/individuels	Taux de satisfaction des supérieurs hiérarchiques
4	Evaluation du risque spécifique	Contribution à la stratégie
5	Risque (taux de crise sur le risque, actualisation du catalogue de risque)	Respect du budget

Source : AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p23.

- Risk manager catégorie « Assurance et Prévention, *AP* », les critères comprennent :

Tableau N°8 : Les critères qualitatifs et quantitatifs de la performance du Risk Manager catégorie « AP »

	AP	
	Critères quantitatifs	Critères qualitatifs
1	Objectifs groupe	Objectifs
2	Budget	Prévention
3	Productivité des process de gestion	Relations
4	Performances groupe/individuelles	Innovation
5	Efficacité de la prévention	Communication et compréhension des guidelines

Source : AMRAE; Le baromètre de Risk Manager; 2011; op.cit; p23.

Nous pouvons résumer que la fonction de risk manager relève un poste très complexe pour un profil multidisciplinaire qu'il est aussi bien compliqué. Comme le dit C.Aubry et M.A.Montalan, un idéal Risk manager doit être à la fois un financier, un technicien, modélisant du risque, un ingénieur, définissant des procédures, négociateur, juriste et un manager[*].

Nous joindrons aux annexes (voir annexe N°2) un descriptif du fiche de poste type[1], illustrant les responsabilités, les activités spécifiques et les compétences professionnelles nécessaires à la fonction du risk manager.

[*] Plus amples du détail sur le profil, les qualités et les formations liées au Risk Manager nous renvoyons le lecteur intéressé vers l'ouvrage de Catherine Véret et Richard Mekouar « Fonction : Risk manager », ainsi au baromètre AMRAE du Risk Manager, 2011.

[1] AMRAE; Fiche Métier RISK MANAGER (Gestionnaire des Risques); AMRAE APEC Public; 21/06/2012; http://www.amrae.fr/

Conclusion

A travers ce chapitre, nous avons présenté les notions élémentaires nécessaires à la compréhension du risk-management. Nous avons tiré plusieurs préceptes, parmi lesquels nous citons que:

Les entreprises sont actuellement confrontées à des nouveaux défis et à problèmes croissants dus à la complexité, l'incertitude, l'extrême concurrence de l'environnement économique, industriel et social, ainsi que des difficultés rencontrées dans le management de leurs projets. C'est pourquoi le management du risque est devenu pour beaucoup d'entreprise une préoccupation majeure.

La mise en œuvre efficace du risk management aide les organisations à se conformer aux exigences des lois et règlements et aux normes internationales pertinentes. Le processus de risk management établie une assise fiable pour la prise de décisions et la planification, ce qui englobe l'affectation adéquate des ressources à l'ensemble du processus.

Les principes régissent le processus de risk management, établissent les valeurs et la philosophie sous-tendant le processus. Ils appuient une vision complète et coordonnée du risque qui s'applique à l'ensemble de l'organisation. Les principes de risk management lient le cadre et la pratique du management du risque aux objectifs stratégiques de l'entité, ils aident également à harmoniser le risk management et les activités de l'organisation.

Nous sommes en effet convaincus que ce dont nos entreprises ont besoin pour mieux maitriser leurs risques dans un environnement de plus en plus complexe et incertain, ce n'est pas de règlementation supplémentaire mais d'un surcroit d'expertise, de bon outils et de méthodes de travail qui associent plus étroitement la direction générale, ses équipes en charge de la gestion et du contrôle des risques, les auditeurs externes et internes et les membres d'administration.

Par ailleurs, le Risk Manager, responsable de cette fonction, a pour mission d'identifier tous les risques internes et externes, d'élaborer une cartographie des risques afin de les apprécier, ainsi que traiter ces risques en définissant une stratégie du management des risques, et enfin la dernière est de prêter assistance aux managers dans la réalisation de la stratégie. Néanmoins, les compétences du Risk manager peuvent jouer un mauvais tour, il pourra faire des évaluations incorrectes, cela mènera à des allocations de ressources inadéquates.