Chapitre 2 : Le déploiement du Risk management et l'évaluation de son efficacité

Mettre en place une politique de management du risque est devenue nécessaire de nos jours, et surtout dans ces temps de crise pour que chaque organisation puisse être capable de maîtriser ses activités. Toutefois, dans la recherche d'une efficacité maximale, cette maîtrise doit passer forcement par une meilleure connaissance des risques auxquels elle est confrontée.

L'approche de management du risque demeure dans la plupart des entreprises plus qualitative (un atelier d'évaluation par des méthodes qualitatives) que quantitative (puissants outils analytiques) et la cartographie des risques est l'outil central de l'anticipation de ces risques.

Donc notre chapitre qui est représenté en trois sections, portera en premier lieu (1ère section) sur la cartographie des risques comme base du processus Risk Management et les préalables à son élaboration. Nous avons présenté comment le management du risque apprécie les risques d'entreprise et quel est le processus pour se faire. Ce processus qui passera par l'identification des risques, l'analyse de ces risques et leur évaluation et hiérarchisation, doit être traité et surveillé en élaborant une revue du processus Risk Management.

Dans la deuxième section, nous avons démontré comment les méthodes et les techniques d'analyse des risques seront sélectionné et classifié selon des approches connues comme l'approche déterministe et l'approche probabiliste, ainsi que l'approche qualitative et quantitative. Le choix de ces méthodes est mis en œuvre selon des critères et facteurs définis par l'entreprise. Cependant, plusieurs méthodes étaient mises en évidence dans cette section dans un panorama divisé en deux parties: les méthodes qualitatives et les méthodes quantitatives, nous avons ensuite comparé ces méthodes un par un, par rapport à leur applicabilité, aux critères de leur qualité et aux facteurs influençant leur choix.

La troisième section porte sur l'audit interne et son rôle dans l'évaluation de l'efficacité du management du risque. Elle commence par les objectifs de l'audit du management du risque et les caractéristiques pour un système efficace de contrôle interne et management du risque. Ensuite, nous présenterons la revue de management du risque par l'audit interne, et nous terminerons notre section par l'assurance sur le processus de management du risque.

Section 1 : La cartographie des risques comme base du processus risk management

Dans un souci de généralisation, notre étude regroupera des cycles définis dans des normes et cadres référentiels de management du risque. Dans le but d'orienter notre choix, on procède a une comparaison des différents cycles de processus Risk Management dans le Tableau ci-dessous ou chaque colonne représente un cycle étudié.

Tableau N°09: comparaison des différents cycles de processus Risk Management

Généralisation	ISO 31000	COSO II, 2004	AS/NZS 4360 : 2004	AIRMIC et al, 2002 & FERMA,2003
Phase préalable	Établissement du contexte	l'environnement interne		structurer et superviser le MR
		Fixation des objectifs	Prise en compte du contexte	définir les objectifs stratégiques
Identification des risques	Appréciation du risque : - Identification du risque - Analyse du risque - Évaluation du risque	Identification des événements	Estimation du risque: - Identifier - Analyser - Évaluer	Appréciation du risque: - Analyser (identification, description, estimation) - Évaluation du risque
Analyse et évaluation des risques		Évaluation des risques		Compte-rendu sur le risque
Traitement des risques	Traitement du risque	Traitement du risque		Décision
			Traitement du risque	Traitement du risque
				Compte-rendu sur le risque résiduel
Suivi et améliorer le processus RM	Communication et Concertation Surveillance et revue	Activités de contrôle	Suivre et réviser	Suivi du risque
		Information er Communication	Communiquer et consulter	
		Pilotage	Pilotage et revue	

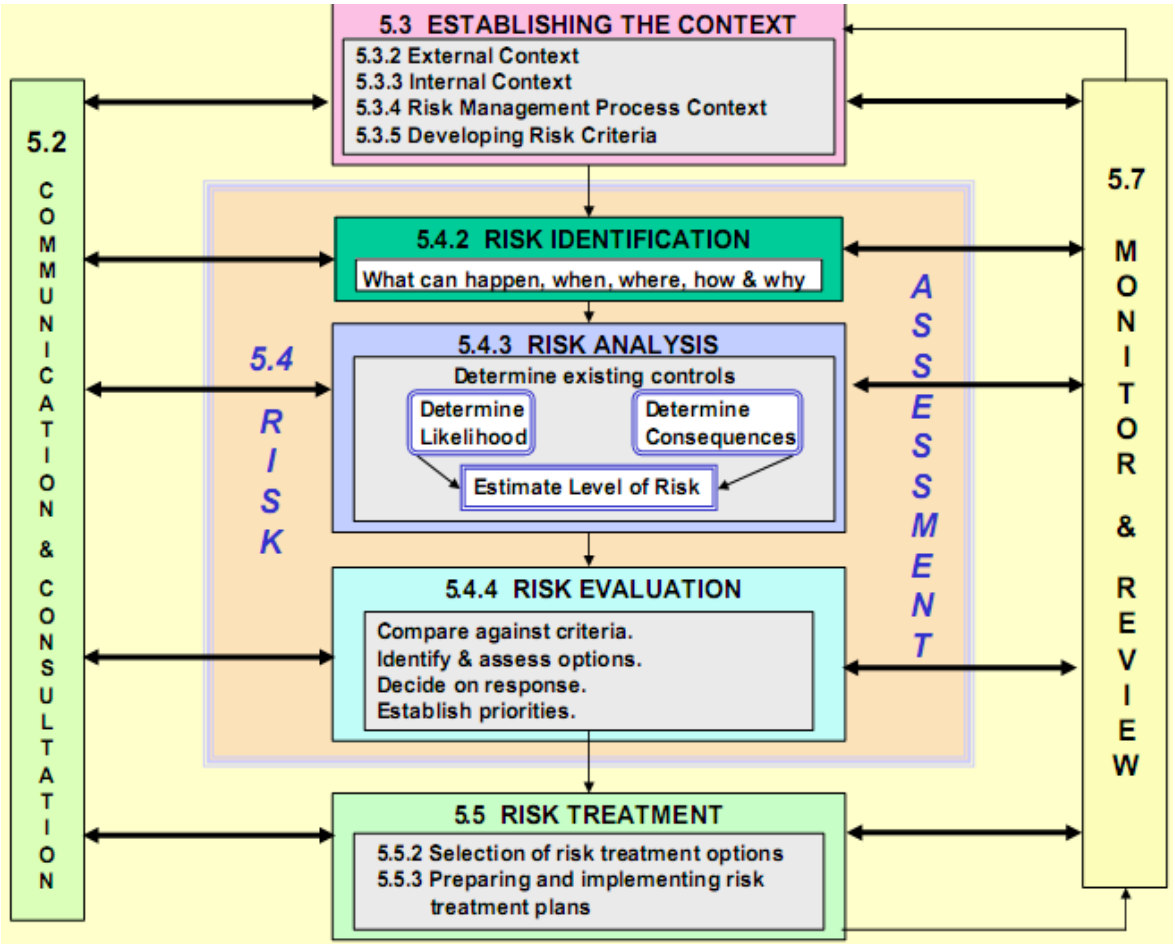
Source : préparé par l'étudiante.

Les étapes définies dans différentes approches de management du risque sont quasi homogènes, malgré la différence des termes qui les désignent. La première colonne montre que, d'une manière générale on distingue une première étape de cadrage a travers laquelle les objectifs, l'environnent et le planning du processus de management du risque seront établis. A cela s'enchaine une phase opérationnelle consistant en l'identification, l'analyse, l'évaluation, le traitement et le suivi des risques. Dans d rares cas, comme celui de COSO-II et ISO 31000, le processus de management du risque se termine par une phase d'évaluation dans une vision d'améliorations de sa performance.

En outre, ces normes regroupent les étapes d'identification, d'analyse et d'évaluation des risques en une macro-étape, qui se dénomme " *appréciation des risques* ".

L'ISO 31000 présente le plus récent des cycles de management des risques étudie jusqu'ici. Ce dernier semble incorporer les autres cycles1. En plus, la norme prévoit un cadre de management et d'améliorations du cycle de management du risque, et un ensemble de méthodes d'appréciation des risques (ISO/IEC 31010).

Figure N°23 : Le processus Risk Management selon ISO 31000



Source: Kevin W. Knight; transitioning to the new risk management standard AS/NZS/ISO 31000:2009

Le cycle de management propose dans la norme ISO 31000, semble ainsi être pertinent pour le management du risque car, il présente un haut degré de généricité dans ce sens qu'il a une forte similitude avec les étapes de la première colonne du Tableau N°09.

1. Préalables à l'élaboration de la cartographie des risques : Établissement du contexte

Le processus de management du risque débute par une phase d'étude préalable en établissant le contexte, l'organisation énonce clairement ses objectifs, définit les paramètres internes et externes à prendre en compte dans le management du risque, et détermine le domaine d'application et les critères de risque pour la suite du processus. Bien que la plupart de ces paramètres soient semblables à ceux pris en compte dans la conception du cadre organisationnel de management du risque pour l'établissement du contexte du processus de management du risque.

[1] Kevin W. Knight; transitioning to the new risk management standard AS/NZS/ISO 31000:2009 ;Cprm; Hon Frmia; Firm (Uk); Lmrmia; chairman ISO working group -risk management standard; member standards australia / standards new zealand; joint technical committee ob/7 -risk management; august 2009; p37.

Dans ce cadre, les objectifs d'évaluation des risques, les critères de risques et le programme de maîtrise des risques sont déterminés et font l'objet d'un accord visant à[1] :

- Choisir les intervenants clés et fixer les modalités de l'étude (statut et rôle des participants, disponibilité, etc) ;

- Déterminer l'approche à utiliser « Top-down ou Bottom-up » ;

- Fixer le champ et le planning de l'étude ;

- Décrire les processus (mandat, objectifs, enjeux, préoccupations, environnement interne et externe, intrants, extrants, ressources et macro-processus) ;

- Identifier les risques en lien avec les objectifs ;

- Utiliser une terminologie commune et choisir les techniques et outils à adapter.

1.1. L'établissement du contexte interne et externe [2]

L'établissement du contexte externe implique de se familiariser avec l'environnement externe dans lequel l'organisation cherche à atteindre ses objectifs et évolue. En fait, il est important de comprendre le contexte externe afin de s'assurer que les objectifs et les préoccupations des parties prenantes externes sont pris en compte lors de l'élaboration des critères de risque. Le contexte externe est basé sur le contexte à l'échelle de l'organisation, avec toutefois des détails spécifiques découlant des obligations légales et réglementaires, des perceptions des parties prenantes et d'autres aspects des risques propres au domaine d'application du processus de management du risque.

Le contexte externe peut inclure, sans que la liste soit exhaustive :

- L'environnement social et culturel, politique, 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'organisation ;

- Les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

En outre, Il convient que le processus de management du risque soit cohérent avec la culture, les processus, la structure et la stratégie de l'organisation. Le contexte interne comprend tout ce qui, au sein d'une organisation, peut influencer la manière de maîtrise des risques. Il convient de l'établir car :

- Le management du risque se fait dans le contexte des objectifs de l'organisation ;

- Il convient d'envisager les objectifs et les critères d'un projet, d'un processus ou d'une activité spécifique à la lumière des objectifs de l'organisation dans leur ensemble ;

- Et certaines organisations ne parviennent pas à identifier les opportunités leur permettant d'atteindre leurs objectifs en matière de stratégie, de projet ou d'activité, ce qui compromet la continuité de l'engagement, de la crédibilité, de la confiance et des valeurs de l'organisation.

[1] Serge Bédard, Adm.A, CISA, CISM; La gestion intégrée des risques d'entreprise, de la théorique à la pratique; Présentation faite par la communauté de pratique en gestion de projets publics au Québec ; Mercredi le 3 mars 2010; p 15.
[2] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit ; p 16.

Il est nécessaire de comprendre le contexte interne. Cela peut inclure, sans toutefois s'y limiter [1]:

- La structure de l'organisation (gouvernance, les rôles et les responsabilités) ;
- Les politiques, les objectifs et les stratégies mises en place pour les atteindre ;
- Les aptitudes, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies ;
- Les relations avec les parties prenantes internes, leurs perceptions et leurs valeurs, ainsi que la culture de l'organisation ;
- Les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels) ;
- Les normes, principes directeurs et modèles adoptés par l'organisation ;
- La forme et l'étendue des relations contractuelles.

1.2. Établissement du contexte du processus Risk management et définition des critères de risque[2]

Il convient de fixer les objectifs, les stratégies, les domaines d'application et les paramètres des activités de l'organisation où le processus de management du risque s'applique. Il convient d'entreprendre le management du risque en tenant compte de la nécessité de justifier les ressources servant à sa mise en œuvre. Il convient également de spécifier les ressources nécessaires, les responsabilités et autorités ainsi que les enregistrements à conserver.

Le contexte du processus de management du risque varie selon les besoins de l'organisation. Il peut inclure, sans toutefois s'y limiter ce qui suit :

- La définition des buts et des objectifs des activités de management du risque ;
- La définition des responsabilités relatives au processus de management du risque ;
- La définition du domaine d'application ainsi que le degré et l'étendue des activités de management du risque à entreprendre, y compris ce qui est spécifiquement inclus et exclu ;
- La définition de l'activité, du processus, de la fonction, du projet, du produit, du service ou de l'actif en termes de temps et de lieu ;
- La définition des relations entre un projet, un processus ou une activité donnée et les autres projets, processus ou activités de l'organisation ;
- La définition des méthodes d'appréciation du risque ;
- La définition de la méthode selon laquelle les performances et de l'efficacité du management du risque sont évaluées ;
- L'identification et la spécification des décisions à prendre, et
- L'identification, le domaine d'application ou le cadre organisationnel des études requises, leur étendue et leurs objectifs, ainsi que les ressources nécessaires à leur réalisation.

La prise en compte de ces facteurs et des autres facteurs pertinents permette de s'assurer que l'approche de management du risque retenue est adaptée aux circonstances, à l'organisation et aux risques affectant l'atteinte de ses objectifs.

[1] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit; p 16.
[2] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit; p 17.

Toutefois, la définition des critères de risque comprend [1]:

✓ La nature et les types de causes et de conséquences qui peuvent survenir, et la manière de les mesurer ;

✓ La méthode de définition de la vraisemblance ;

✓ L'échelle de la vraisemblance et/ou de la (des) conséquence(s) ;

✓ La méthode de détermination du niveau de risque ;

✓ Les avis des parties prenantes ;

✓ Le niveau à partir duquel le risque devient acceptable ou tolérable ;

✓ La prise en compte ou non des combinaisons de plusieurs risques et, le cas échéant, la méthode à utiliser et les combinaisons à considérer.

Certains critères peuvent être imposés ou résulter d'obligations légales et réglementaires, ou d'autres exigences auxquelles l'organisation répond. Ces critère doivent être définis au début de tout processus de management du risque et soient revus continuellement.

1.3. L'approche Top-Down « descendante » et Bottom-Up « ascendante »

Après avoir établir le contexte du processus de management du risque, et avant de commencer l'élaboration d'une cartographie des risques, il faut tout d'abord déterminer son périmètre dans l'organisation et retenir une de deux approches, globale ou détaillé, pour planifier les différentes étapes de la démarche. Il faudra que l'organisation décide à quel niveau doit être effectué la cartographie des risques ?

Tout dépend bien évidemment de la taille de l'organisation, de ses diverses implantations et de son portefeuille d'activité. Il ne s'agit pas de multiplier les cartographies sans cohérence avec les besoins de maîtrise des risques de l'entreprise. Il faut donc raisonner en termes d'utilité et de coûts / avantages pour décider de mettre en place une telle démarche. Précisons d'emblée que nous parlons ici d'une cartographie dite « ***globale*** » et qui a pour but de recenser l'ensemble des risques majeurs de l'entreprise qui peuvent être de nature très variée, contrairement à une cartographie dite « ***thématique*** », focalisée sur un seul process, une activité ou un seul secteur de l'entreprise.

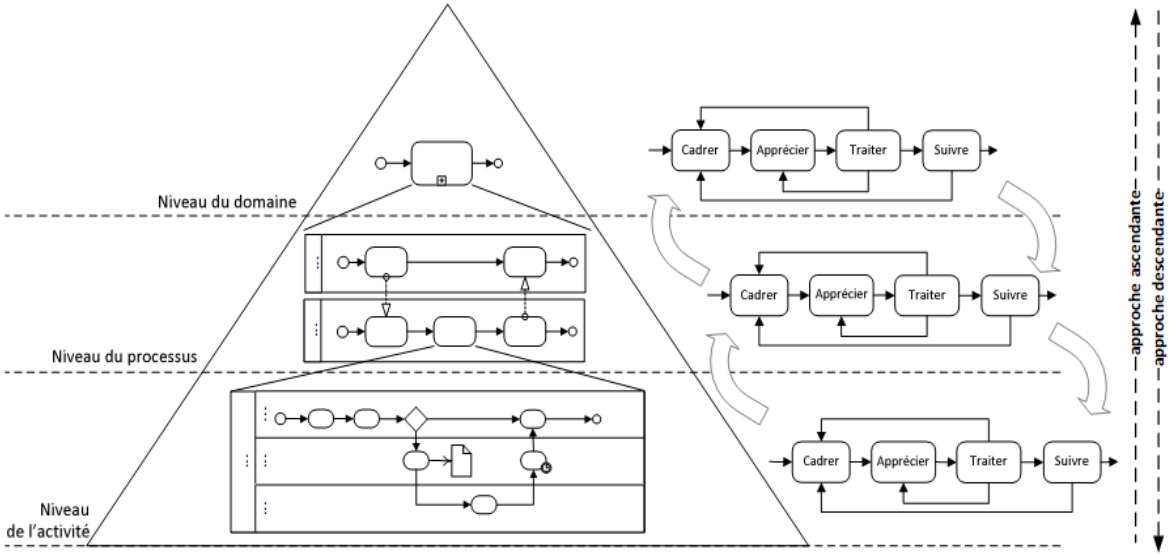
En cours de conception de la cartographie des risques, cette démarche peut s'interpréter selon une approche descendante « ***Top-Down*** » ou selon une approche ascendante « ***Bottom-up*** » en fonction de la granularité des activités de l'entreprise.

L'approche Top-Down est l'application de la démarche à un domaine, puis à ses processus et en descendant successivement jusqu'aux activités. Elle est probablement plus adaptée quant on se situe dans un contexte nouveau. Si l'on dispose déjà d'un ensemble d'activités bien connues en termes de risque, on préférera une démarche bottom-up. Pour cela, on commencera l'étude au niveau d'un ensemble d'activités pour l'agréger successivement aux processus formés par celles-ci, pour aboutir à une agrégation en domaines[2].

[1] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit; p 17.

[2] Amadou Sienou; Op.cit; p 116.

Figure N°24 : L'approche Top-Down « descendante » et Bottom-Up « ascendante »



Source : Amadou Sienou; op.cit; p 117.

Bien entendu, les deux approches s'opposent pour faire circuler l'information au sein de l'entreprise. Ainsi, soit l'information suit un circuit part des hautes instances de l'organisation pour être diffusée entre les différents services, soit l'information suit un circuit Bottom-Up où l'information est progressivement remontée des plateformes opérationnelles jusqu'à la Direction Générale. Ces deux approches sont également transposées dans la démarche de la cartographie des risques

L'approche Bottom-Up est la plus utilisée pour mettre en place la cartographie des risques. Le risk manager analyse chaque processus de l'entreprise pour faire ressortir méthodologiquement les risques majeurs. Dans une démarche de cartographie globale, cette approche est pertinente puisqu'il s'agit de rencontrer les personnes qui sont les plus proches des opérations et qui sont donc le plus à même d'être confrontées quotidiennement aux risques. Puis, le risk manager porte à la connaissance des personnes en charge les risques de terrain identifiés par les opérationnels. Selon Gilbert de Mareschal[1], l'identification des risques se fait de manière relativement libre et ouverte ; Elle se fait donc par entretiens ou lors d'ateliers avec les opérationnels, des membres des fonctions support (marketing, ressources humaines, systèmes d'information) en utilisant une grille des risques potentiels, préparée à l'avance, afin de s'assurer que tous les risques ont bien été évoqués. Puis, une synthèse des risques majeurs est présentée aux dirigeants qui les valident et les hiérarchisent.

Tandis que, avec l'approche descendante l'identification des risques majeurs est préalablement faite par une analyse du risk manager qui doit envisager les principaux risques de l'entreprise pour chaque partie prenante. Ensuite, le risk manager doit alors resituer ces risques, les rattacher au sein des processus de l'entreprise.

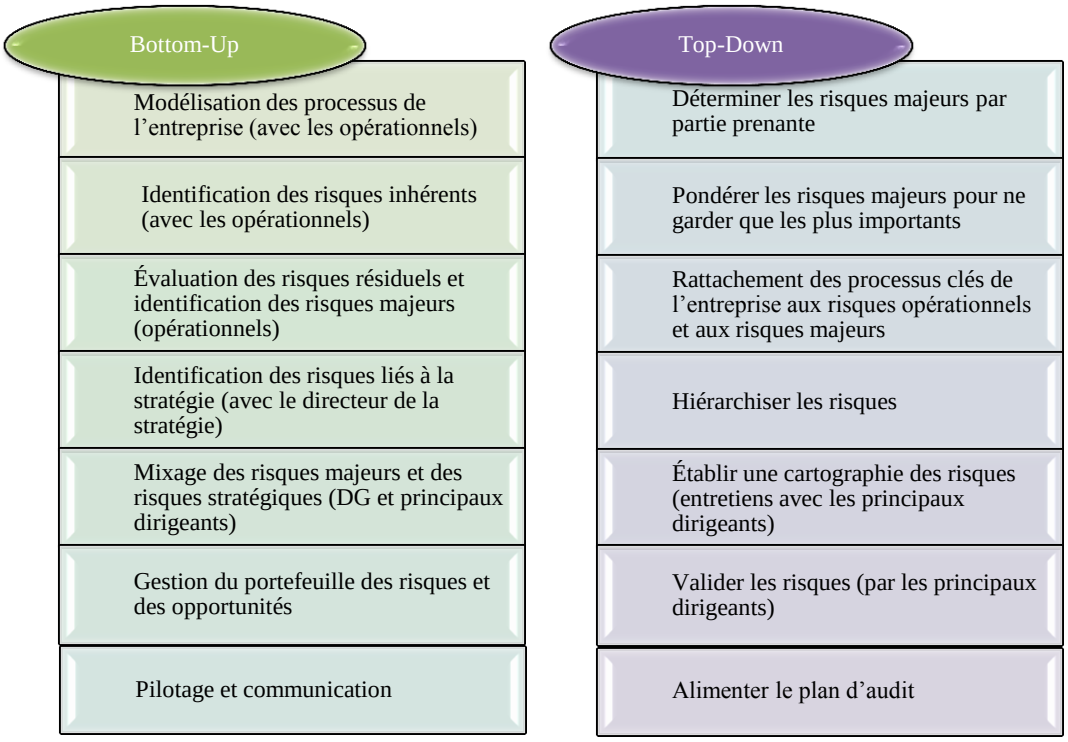
Cette approche « Top-Down » relève une méthode d'identification des risques plus fermée dans le cas d'une cartographie globale. Elle est plus souvent utilisée dans une cartographie thématique, où le risk manager limite ses recherches à un domaine, un métier, ou une géographie particulière.

[1] Mathieu Girème; La formalisation du processus de management des risques à travers l'élaboration d'une cartographie des risqeus; Mémoire de professionnalisation : Master 2; Direction Financière, Contrôle de gestion et Audit interne; IAE Bordeaux; Septembre 2011; p34.

Dans ce cas, l'évaluation et la validation des risques se fait lors des entretiens avec les principaux dirigeants. Si toute l'information n'est pas obtenue lors de ces entretiens, cela oblige à aller chercher davantage d'information auprès des acteurs plus proches de ces risques spécifiques. Le succès de cette approche repose donc sur la capacité initiale du risk manager à cerner les risques majeurs lors de son travail de recherche.

En résume, il faut retenir que les deux approches « Top-down et Bottom-Up » comportent différentes étapes incluant ce qui suit[1] :

Figure N°25 : Comparaison des approches « Top-Down Versus Bottom-Up »



Source : IFACI; Étude du processus de management et de cartographie des risques; Op.cit; 2003; p27; 35.

Ces deux approches sont très certainement complémentaires et il n'existe pas d'approche meilleure, car certains risques importants seront facilement décelés par une vision d'ensemble au niveau de la direction, et d'autres par la connaissance approfondie des opérationnels. Le défi est de réunir les deux approches.

Toutefois, ce cloisonnement des approches demeure relativement conceptuel. Il est illusoire de croire qu'une de deux méthodes doit être à terme entièrement privilégiée. En effet, si une doit prévaloir lors de l'élaboration de la cartographie des risques, une fois mise en place le processus de la maîtrise des risques est heureusement un mélange de ces deux approches. Le management du risque doit être interactif entre les hauts dirigeants et les risk owners. Ces derniers surveillent les risques existants, signalent les risques potentiels et établissent le reporting qui est présenté aux dirigeants. Quant aux dirigeants, ils fixent les objectifs de management du risque et s'assurent son déploiement. Cet apprentissage et cet échange réciproque ne peuvent être que bénéfiques pour la maîtrise des activités de l'entreprise et les acteurs qui y participent.

[1] IFACI; Groupe professionnel Industrie et Commerce; Étude du processus de management et de cartographie des risques; Les cahiers de recherche de l'IFACI; 2003; p27; 35.

2. L'appréciation des risques d'entreprise : Risk Assessment

Dans la Figure N°23, le modèle du processus Risk Management selon l'ISO 31000, révèle sept étapes principales dont les trois phases, de l'identification, l'analyse et l'évaluation des risques, se laissent regrouper en une macro-étape dénommée « *l'appréciation des risques* », nous les présenterons ci-après.

2.1. L'identification des risques

La première étape de la phase d'appréciation des risques consiste à identifier les sources de risque, les domaines d'impact, les événements, y compris les changements de circonstances, ainsi de déterminer leurs causes et conséquences potentielles. Cette étape a pour objectif de dresser une liste exhaustive des risques basée sur les événements susceptibles de provoquer, de stimuler, d'empêcher, de gêner, d'accélérer ou de retarder l'atteinte des objectifs. Il est important d'identifier les risques associés au fait de ne pas saisir une opportunité. Il est essentiel de procéder à une identification exhaustive, car un risque non identifié à ce stade ne sera pas inclus dans une analyse ultérieure[1].

La phase de l'identification vise la description des risques, ainsi elle consiste à étudier les différents aspects du système et à établir des scénarios mettant en évidence des risques potentiels. Cette phase comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentiels ; aussi bien, l'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis des experts et autres personnes compétentes et tenir compte des besoins des parties prenantes[2].

L'identification est une étape cruciale qui mobilise plusieurs techniques telles que la méthode des interviews, les bases de connaissances, des inventaires, des ateliers, des entretiens et des analyses des flux de processus, etc.

Cette phase du processus est opérationnalisée par le risk manager en collaboration avec les experts du domaine qui contribueront à la caractérisation des risques significatifs, en précisant si possible tout ce qui peut se produire, et examiner les causes possibles et les scénarios des conséquences éventuelles.

Toutefois, O.J.Nguén souligne que l'identification des risques pourra se mener selon six directions, à savoir[3] :

- Par les ressources affectées (techniques, informationnelles, économiques, financières, partenariales et environnementales) ; ici, l'important étant de déceler la possibilité d'indisponibilité d'une ressource et de son impact sur l'atteinte des objectifs de l'entreprise, en analysant les éléments qui suivent[4] :

  - Le personnel ;
  - Les matières ;
  - Les équipements ;
  - Les installations ;
  - La chaine logistique ;
  - Les flux d'information ;
  - Les moyens de communication tant interne qu'externe ;

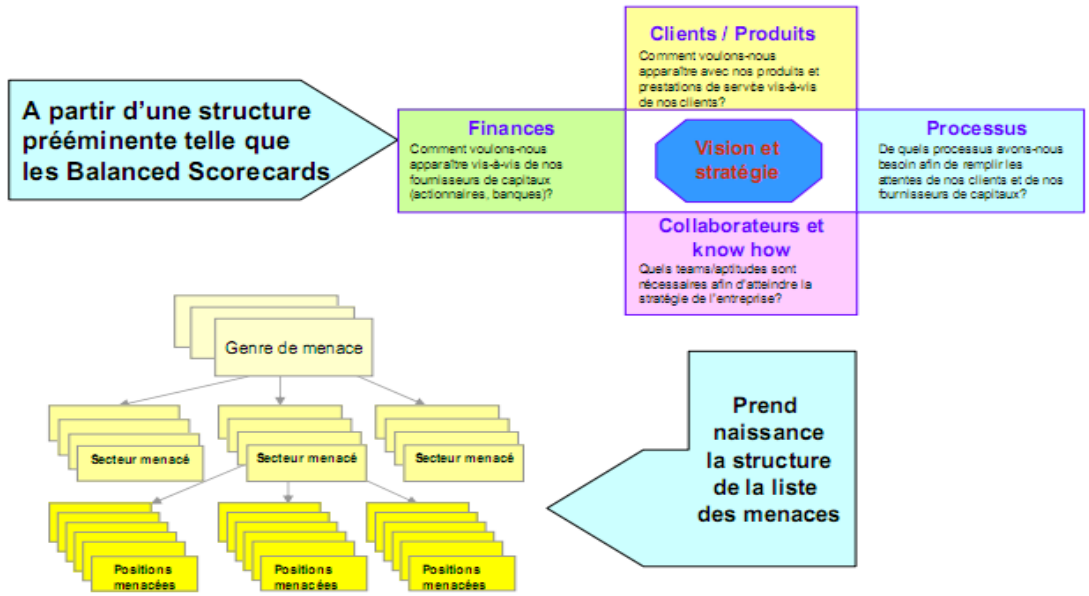
[1] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit; p18.
[2] ISO/IEC guide 73; Op.cit; p5.
[3] Octave Jokung Nguén; Op.cit ; p 61.
[4] Idem ; p 62.

- Les besoins techniques et finances en cas de crise ;
- Les flux financiers ;
- Les utilités telles que l'air, la terre et l'eau.

- Par les objets de risques ;
- Par les conséquences ;
- Par les causes;
- Par la méthode des centres ;

Ici, l'entreprise est abordée en tant que mosaïque de centre d'activités présentant chacun des objectifs propres qui découlent de l'application de la direction participative par objectifs[1]. Ce faisant, le résultant des objectifs de l'ensemble des centres correspond en principe aux objectifs de l'entreprise. Un centre d'activité est une entité au sein de l'entreprise dotée de ses propres objectifs, possédant des ressources idoines ainsi qu'un certain degré d'autonomie et un responsable à sa tête.

Figure N°26 : Identification des risques par la méthode des centres

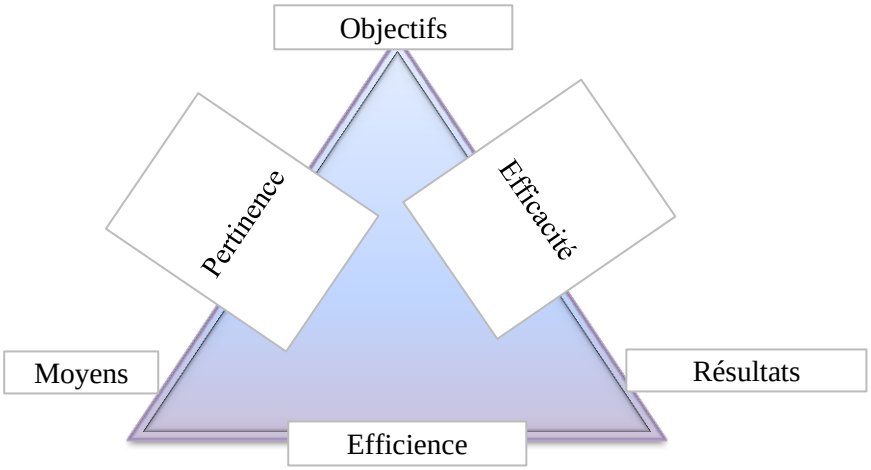


Source: ON 49000: La gestion du risque pour les organisations et les systèmes-Ligne directrices; SQS-EuroRisk; p24.

O.J.Nguén ajoute que le principe du triangle d'Or s'applique intégralement car le centre sera évalué sur sa pertinence (adéquation entre les moyens et les objectifs), son efficacité (atteinte des objectifs assignés) et son efficience (usage à bon escient des moyens mis à sa disposition), comme figuré ci-après :

[1] ON 49000: La gestion du risque pour les organisations et les systèmes-Ligne directrices; SQS-EuroRisk; p24.

Figure N°27: Le triange d'Or



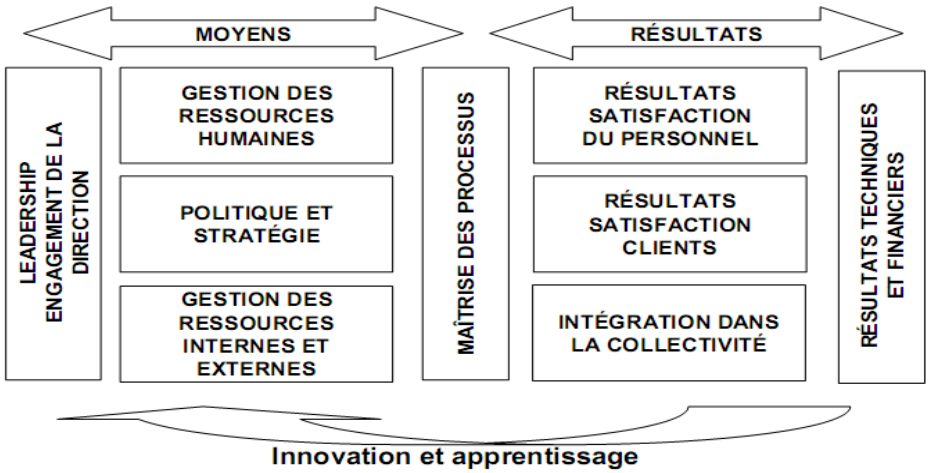
Source : Octave Jokung Nguén; Op.cit ; p 65.

Le préalable de cette méthode consiste en l'identification des centres d'activités en s'appuyant sur la définition précédente. Font de la connaissance desdits centres et de leurs responsables, les risques seront analysés au niveau de chaque centre. Chaque centre possédant en effet un objectif est une déclination des objectifs généraux de l'entreprise. Il est question ici de mettre en exergue l'ensemble des risques qui en affectant en péril l'entreprise.

Cette analyse se déroulera sous forme d'entretien avec le responsable du centre d'activités et de visites sur le site. Un rapport sera aussitôt rédigé et partagé avec les membres du centre concerné[1].

En outre, le modèle Le modèle d'excellence de l'EFQM [2]« European Foundation for Quality Management », est un outil permettant de représenter les différents centres d'activités de l'entreprise de façon complète, selon neuf « 9 » critères, comme suit :

Figure N°28 : Le modèle d'excellence de l'EFQM



Source : Yves Métayer, Laurence Hirsch; Op.cit ; P 37.

Les critères situés à gauche concernent les moyens que l'entreprise déploie pour assurer sa performance actuelle, mais aussi pour garantir son développement futur. Les critères situés à

[1] Octave Jokung Nguén; Op.cit ; p 65.
[2] Yves Métayer, Laurence Hirsch; Op.cit ; P 36-37.

droite permettent d'évaluer la performance de l'entreprise vis-à-vis de l'ensemble de ses parties prenantes.

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

⊕ Par les processus ;

Le point d'ancrage de cette approche réside dans la description des processus mis en œuvre au sein de l'entreprise et par celle des activités liées auxdits processus, cette description passe par les étapes suivantes[1] :

- Détermination de l'intitulé du processus ;
- Définition du but et de la raison d'être ;
- Identification du ou des domaines dans lequel il est mis en œuvre ;
- Identification des intervenants ou acteurs ;
- Détermination de leurs rôles ;
- Détermination des conditions de déclenchement ;
- Description chronologique des actions ;
- Identification des flux d'information : données d'entrées, de sorties ;
- Définition des conditions de fin du processus ;
- Établissement des interactions potentielles avec d'autres processus ;
- Détermination des outils et documents associés.

Un processus doit par essence être permanent, regrouper un ensemble d'activités ayant en commun l'élaboration d'un produit ou un service et être descriptible par un diagramme temporel de flux.

Les processus seront scindés en trois catégories en recourant au concept de chaîne de valeur Porter[2] :

➲ ***les processus stratégiques*** : définissent la stratégie globale de l'entreprise, son pilotage et sa communication ;

➲ ***les processus métiers ou primaires*** : s'intéressent à la production la logistique, l'approvisionnement, la conception et à la vente ;

➲ ***les processus supports ou secondaires*** : définirent les ressources humains (recrutement, gestion de carrière, formation, etc), s'intéressent au processus d'amélioration, assurèrent le financement de l'entreprise, son contrôle de gestion ainsi que la maîtrise des risques.

Par ailleurs, O.J.Nguén évoque que l'approche par les centres se rapproche de celle basée sur les processus. Or, la première s'intéresse aux centres d'activités et n'analyse pas leurs interactions tandis que l'approche par processus en ne circonscrivant pas le déploiement des processus permet d'aller au-delà des centres et autorise ainsi l'analyse des liaisons existant entre lesdits centres. Par nature transversale, l'approche par les processus complétera à bon escient celle des centres.

[1] Yves Métayer, Laurence Hirsch; Op.cit ; P 63.
[2] Octave Jokung Nguén; Op.cit ; p 66.

In fin, l'objectif de cette première étape d'appréciation des risques est l'exhaustivité d'identification des risques les plus significatifs et pertinents ; la recherche de cette exhaustivité peut prendre appui sur la description des processus et des activités mises en œuvre dans l'entreprise. Or, l'approche systémique répond mieux à cette attente compte tenu que l'entreprise que être appréhendée comme un système ouvert, recevant des inputs et générant des outputs, tout en étant en interaction avec son environnement mais en sus soumis à des forces interne. C'est cette approche qu'il faudra privilégier tout en considérant les spécifiés de l'entreprise impétrante.

On résume que l'identification des risques est un processus systémique de recherche, de reconnaissance et d'enregistrement des risques, en respectant un ensemble de principes qui sont la cohérence entre les techniques d'identification des risques, les objectifs et les aptitude de l'entreprise, la couverture du périmètre d'étude, l'actualité de l'information relative aux risques, la prise en compte du degré de contrôle sur les risques et de la résistance possible des acteurs[1].

2.2. L'analyse des risques[2]

L'analyse des risques consiste à comprendre et à étudier profondément les risques. Elle constitue une donnée d'entrée de l'évaluation des risques et dans la prise de décision sur la nécessité de traiter les risques et sur les stratégies ou méthodes de traitement les plus appropriées.

L'analyse des risques consiste à déterminer les conséquences et les probabilités pour les risques identifiés en tenant compte de la présence (ou non) et de l'efficacité des contrôles existants. Probabilité et conséquence associée sont alors combinées pour déterminer le niveau de risque.

L'analyse des risques implique de tenir compte des causes et des sources du risque ainsi que de leurs conséquences et de la probabilité de leur occurrence. Il convient d'identifier les facteurs ayant un effet sur les conséquences et la probabilité. Un événement peut avoir plusieurs conséquences et peut affecter plusieurs objectifs. Il convient de tenir compte des contrôles de risque existants et de leur efficacité. Différentes méthodes d'analyse sont présentées dans la section deux. Pour des applications complexes, il peut se révéler nécessaire d'appliquer plusieurs techniques.

En règle générale, l'analyse des risques comprend une estimation de l'ensemble des conséquences potentielles susceptibles de résulter d'un événement, d'une situation ou d'une circonstance, et des probabilités associées, afin de mesurer le niveau de risque. Cependant, dans certains cas, par exemple lorsque les conséquences sont probablement négligeables ou que la probabilité prévue est extrêmement faible, il peut être suffisant de n'estimer qu'un seul paramètre pour prendre une décision.

Dans certaines circonstances, une conséquence peut résulter d'un ensemble de différents événements ou de différentes conditions, ou lorsqu'un événement particulier n'est pas identifié. Dans ce cas, l'évaluation des risques porte sur l'analyse de l'importance et de la vulnérabilité des composants du système afin de définir les traitements associés aux niveaux de protection ou aux stratégies de remise en état.

Les méthodes utilisées dans l'analyse des risques peuvent être qualitatives, semi-quantitatives ou quantitatives. Le degré de précision requis dépend de l'application particulière, de la disponibilité de données fiables et des besoins de prise de décision de

[1] Amadou Sienou; Op.cit; p 77.
[2] ISO/IEC 31010; Risk management-Risk Assessment Techniques; International Electro-technical Commission; Geneva; Switzerland; ISO; 2009; p 103.

l'organisation. Certaines méthodes et le degré de précision de l'analyse peuvent être déterminés par la loi.

- ***Évaluation des contrôles existants***[1]

Le niveau de risque dépend de l'adéquation et de l'efficacité des contrôles existants. Cela implique de répondre aux questions suivantes:

- Quels sont les contrôles existants liés à un risque particulier?

- Ces contrôles sont-ils en mesure de traiter le risque de manière à le maintenir à un niveau tolérable?

- Dans la pratique, les contrôles fonctionnent-ils comme prévu et leur efficacité peut-elle être démontrée, le cas échéant?

Il est possible de répondre à ces questions avec certitude uniquement s'il existe une documentation pertinente et si un processus d'assurance adapté a été mis en place.

Le niveau d'efficacité d'un contrôle particulier ou d'une suite de contrôles connexes peut être exprimé de manière qualitative, semi-quantitative ou quantitative. Dans la plupart des cas, un niveau élevé de précision n'est pas garanti. Toutefois, il peut être intéressant d'exprimer et d'enregistrer la mesure de l'efficacité du contrôle des risques de manière à pouvoir émettre un avis sur l'effort à porter pour améliorer le contrôle ou par un traitement différent des risques.

- ***Analyse des conséquences*** [2]

L'analyse des conséquences permet de déterminer la nature et le type d'impact susceptible de se produire, en supposant que des événements ou des circonstances particuliers se sont produits. Un événement peut avoir une série d'impacts de gravité différente et affecter un ensemble d'objectifs et d'acteurs différents. Les types de conséquence à analyser et les acteurs concernés auront été définis lors de l'établissement du contexte.

L'analyse des conséquences peut s'étendre d'une simple description des résultats à une modélisation quantitative détaillée ou une analyse de vulnérabilité.

Les impacts peuvent avoir une conséquence faible mais une probabilité élevée, ou une conséquence élevée et une faible probabilité, ou des résultats intermédiaires. Dans certains cas, il est pertinent de mettre l'accent sur les risques présentant des résultats potentiellement très variés donc faisant souvent l'objet d'une attention particulière de la part des décideurs.

Dans d'autres cas, il peut être important d'analyser les risques à conséquence élevée et faible de manière séparée. Par exemple, un problème fréquent mais à faible impact (ou chronique) peut avoir des effets cumulés ou à long terme importants. Par ailleurs, les traitements appliqués à ces deux différents types de risques sont souvent tout à fait différents, ce qui justifie donc de les analyser séparément.

L'analyse des conséquences peut impliquer :

- De tenir compte de considérations liées aux contrôles existants afin de traiter les conséquences avec tous les facteurs contributifs pertinents ayant un effet sur les conséquences;

- D'associer les conséquences du risque aux objectifs d'origine;

- De tenir compte des conséquences immédiates et de celles susceptibles de survenir ultérieurement, si cela est cohérent avec le domaine d'application de l'évaluation;

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit; p 104
[2] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit; p 104

- De tenir compte des conséquences secondaires comme celles ayant un impact sur les systèmes, activités, équipements ou organisations connexes.

Analyse de la vraisemblance et estimation de la probabilité [1]

Trois approches générales sont couramment utilisées pour estimer la probabilité. Elles peuvent être utilisées individuellement ou conjointement :

➢ ***Utilisation de données historiques pertinentes*** afin d'identifier des événements ou des situations qui se sont produits dans le passé et ainsi extrapoler la probabilité de leur occurrence dans le futur. Il convient que les données utilisées soient adaptées au type de système, d'installation, d'organisation ou d'activité considéré et aux normes de fonctionnement de l'organisation considérée. Si, du point de vue historique, la fréquence d'occurrence est très faible, il peut s'avérer impossible d'estimer la probabilité. Cela concerne particulièrement les occurrences nulles, lorsque personne ne suppose que l'événement, la situation ou la circonstance va se produire dans le futur.

➢ ***Prévision des probabilités à l'aide de techniques prédictives*** telles que l'analyse par arbre de panne et l'analyse par arbre d'événements. Si les données historiques ne sont pas disponibles ou appropriées, il est nécessaire de déduire les probabilités par une analyse du système, de l'activité, de l'équipement ou de l'organisation ainsi que l'échec ou la réussite qui en découle. Les données numériques liées aux équipements, personnes, organisations et systèmes sur la base d'expériences opérationnelles ou de sources de données publiées sont alors combinées pour produire une estimation de la probabilité de l'événement de tête. Lorsque des techniques prédictives sont utilisées, il est important d'assurer que, lors de l'analyse, il a été dûment tenu compte de l'éventualité de défaillance de mode commun qui implique la défaillance de plusieurs pièces ou composants différents du système. Des techniques de simulation peuvent s'avérer nécessaires pour estimer la probabilité de défaillance des équipements et de la structure du fait du vieillissement et d'autres processus de dégradation, en calculant les effets des incertitudes.

➢ *L'avis d'un expert* peut être utilisé dans un processus systématique et structuré pour estimer la probabilité. Il convient que ces avis experts se fondent sur toutes les informations disponibles applicables, y compris les données historiques, spécifiques au système et à l'organisation, expérimentales, de conception, etc. Il existe un certain nombre de méthodes formelles permettant d'obtenir des avis experts qui fournissent une aide à la formulation de questions appropriées. Les méthodes disponibles comprennent l'approche Delphi, les méthodes de comparaison par paires, de catégorisation et de probabilité absolue.

Analyse préliminaire « Dépistage des risques » [2]

Il est possible de procéder à un dépistage des risques pour identifier les risques les plus significatifs, ou pour exclure les risques insignifiants ou mineurs de l'analyse ultérieure.

L'objectif est d'assurer que les ressources sont concentrées sur les risques les plus importants. Il convient de ne pas négliger le dépistage des risques faibles qui surviennent fréquemment et qui ont un effet cumulé significatif.

Il convient que le dépistage repose sur des critères définis dans le contexte. L'analyse préliminaire permet de déterminer l'une des suites d'actions suivantes :

- décision de traiter les risques sans évaluation supplémentaire;
- définition de risques non significatifs collatéraux ne justifiant pas de traitement;

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit; p 105
[2] IDEM; p 106

- poursuite par une évaluation plus détaillée des risques.

Il convient de documenter les hypothèses initiales et les résultats.

Incertitudes et sensibilités[1]

Des incertitudes considérables sont souvent associées à l'analyse des risques. Il est nécessaire de bien cerner ces incertitudes pour interpréter et communiquer de manière efficace les résultats de l'analyse des risques. L'analyse des incertitudes liées aux données, aux méthodes et aux modèles utilisés pour identifier et analyser les risques joue un rôle important dans leur application. L'analyse de l'incertitude implique de déterminer la variation ou l'imprécision des résultats, à la suite de la variation collective des paramètres et des hypothèses utilisés pour définir les résultats. L'analyse de sensibilité est étroitement liée à l'analyse de l'incertitude.

L'analyse de sensibilité implique de déterminer l'importance et la signification du niveau de risque liées à la modification de paramètres d'entrée individuels. Elle permet de distinguer les données qui doivent être précises, de celles qui sont moins sensibles et dont les effets sur l'exactitude générale sont par conséquent moins importants.

Il convient d'établir l'exhaustivité et l'exactitude de l'analyse des risques de manière aussi complète que possible. Le cas échéant, il convient d'identifier les sources d'incertitude et il convient que cela concerne les incertitudes liées aux données et au modèle/méthode. Il convient de définir les paramètres auxquels l'analyse est sensible et le degré de sensibilité.

2.3. L'évaluation et hiérarchisation des risques

L'évaluation du risque consiste à comparer le niveau de risque déterminé au cours du processus d'analyse aux critères de risque établis lors de l'établissement du contexte. Sur la base de cette comparaison, il est possible d'étudier la nécessité d'un traitement.

Dans cette étape d'appréciation des risques, un grand nombre des risques de natures différentes sont identifiés; la phase d'évaluation des risques a pour objet de classer ces risques et de les différencier selon leur acceptabilité.

L'objectif principal de cette phase n'est donc pas tant l'évaluation des risques, mais l'identification d'un seuil d'acceptabilité[2], tenant en considération la tolérance au risque des parties prenantes d'entreprise. Cette étape propose un cadre permettant de comparer les risques et de sélectionner ceux qui devront être traités de ceux qui ne le seront pas sur la base de critères définis lors de l'établissement du contexte[3].

Pour ce faire, il recourt habituellement à une combinaison des méthodes qualitatives et quantitatives. L'impact d'un événement, qu'il soit positif ou négatif, doit être analysé et évalué individuellement ou par catégorie, à l'échelle de l'organisation, tenant en compte à la fois les risques inhérents et les risques résiduels.

Chaque risque étant évalué, le risk manager dresse une cartographie d'un ensemble de risques sélectionnés selon des critères donnés (échelle, nature, cause, conséquence, etc.). La cartographie des risques est un outil qui intervient à plusieurs niveaux pour visualiser les risques par une mise en relation d'au moins deux caractéristiques. Le plus souvent, on utilise une cartographie définie dans les dimensions de probabilité d'occurrence et d'impact dans le but de visualiser la répartition des risques dans différentes zones de gravité (faible, acceptable,

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit; p 106
[2] Marc Fumey; Méthode d'évaluation des risques agrégés; Op.cit; p61.
[3] Robin Taylor and Joanne Lam; Grstion du risques d'entreprise GRE : Une méthode pratique; Conférence présentée par PricewaterhouseCoopers LLP en collaboration avec Deposit Insurance Corporation of Ontario; Jeudi 29 septembre 2011; p13.

non tolérée). Ces zones sont fonctions des critères de risques définis lors de l'établissement du contexte.

➲ ***Les paramètres d'évaluation des risques***[1]

Comme nous avons déjà évoqué chaque risque est défini par deux éléments : l'impact et la probabilité d'occurrence. Ainsi, la cartographie des risques contient deux axes, celui représentant le niveau de l'impact (ou de la gravité) et celui de la probabilité. En multipliant le niveau de gravité par la probabilité on obtient le niveau de criticité d'un risque. Ces trois notions sont chacune évaluée selon une échelle qui leur est propre. Pour chaque échelle, il est préférable de choisir un nombre d'intervalles compris entre trois et cinq. Empiriquement, il est recommandé d'utiliser une échelle à quatre intervalles puisque inconsciemment, la plupart des acteurs tendent à évaluer les risques dans leur valeur moyenne. Choisir une échelle à chiffre pair permet d'éviter cet écueil. Cela incite donc à prendre position, quitte à légèrement sous-estimer ou surestimer un risque.

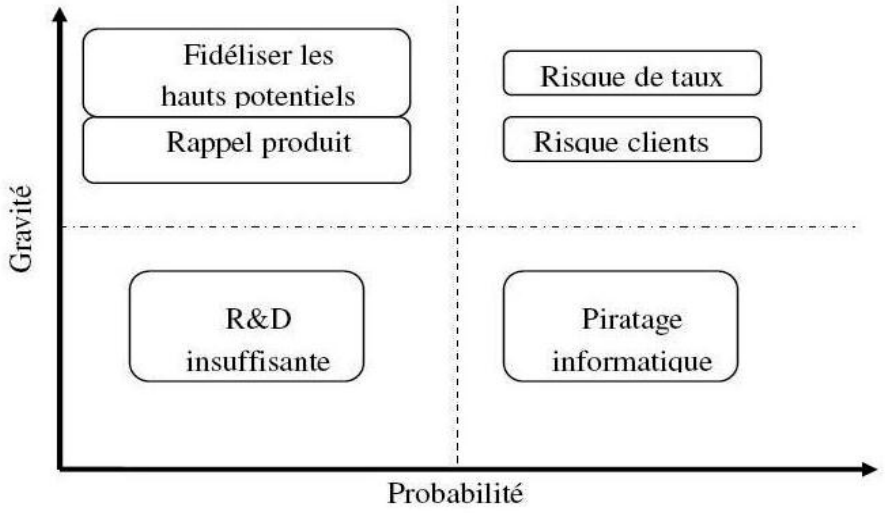
On retiendra généralement deux étapes pour le choix de l'échelle ou les axes d'évaluation des risques.

D'abord, ***La définition des axes*** : il s'agit de choisir entre les couples :

- Probabilité / Gravité ou Occurrence / Impact ;

La figure ci-dessous illustre un exemple d'une cartographie des risques présentée selon le couple Gravité/Probabilité.

Figure N°29: La cartographie des risques selon le couple Gravité / Probabilité



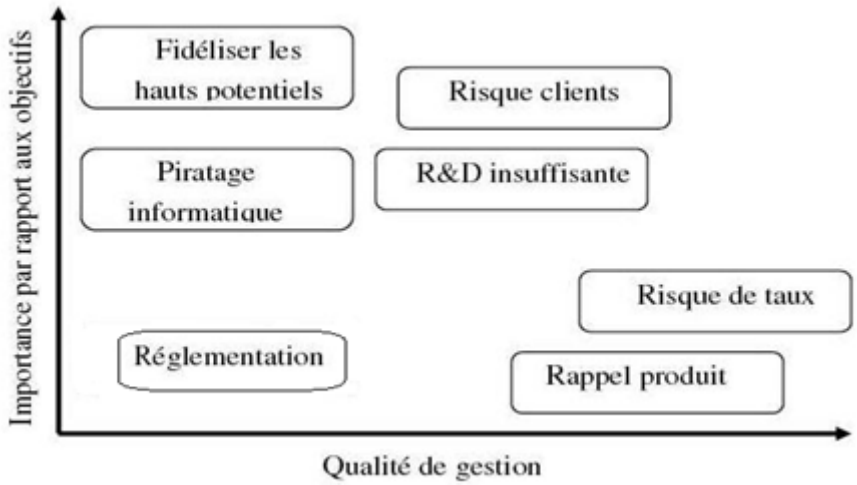
Source: Gilbert Mareschal; la cartographie des risques; Afnor édition; 2003; p38.

De même, la cartographie des risques peut prendre un autre axe d'évaluation des risques.

- Gestion du risque / importance par rapport aux objectifs de l'organisation.

[1] Gilbert Mareschal; la cartographie des risques; Afnor édition; 2003; p38.

Figure N°30: La cartographie des risques selon le couple qualité et gestion / Importance par rapport aux objectifs



Source : Gilbert Mareschal; la cartographie des risques; op.cit; p38.

La réalisation des objectifs stratégiques est mise en avant. L'approche par qualité de gestion/objectifs apporte une vision plus explicite de la performance de l'entreprise puisqu'elle associe directement le degré de maîtrise de l'activité, représenté par la qualité de gestion ou de maîtrise des risques à la réalisation des objectifs.

Cette approche nécessite une forte implication des dirigeants dans la réalisation de la carte car la direction est la seule entité à avoir une vue complète des objectifs de l'entreprise. Aussi, ce mode de fonctionnement donne trop d'importance et de pouvoir aux seuls dirigeants et augmente donc le caractère subjectif de la hiérarchisation des risques.

Le choix des axes est donc un premier paramètre à prendre en compte au regard des différences qu'il apporte dans le résultat final. « Le choix des axes est fonction du type de cartographie, une cartographie synthétique préférera plutôt le couple qualité de gestion/objectifs, alors qu'une cartographie plus précise optera plutôt pour le couple classique probabilité/gravité » précise Gilbert de Maréchal[1].

Dans un deuxième lieu, ***Le choix du type d'axe*** : il s'agit de déterminer le type d'échelle de mesure :

- Qualitatif (bon, moyen, faible) ;
- Semi quantitatif (1, 2, 3, 4) ;
- Quantitatif (pertes engendrées en unité monétaire)

À titre d'exemple nous présentons l'échelle suivant :

- Pour la probabilité : rare, possible, probable, quasi-certain ;
- Pour l'impact : faible, modérée, élevée, critique ;
- Pour la criticité : mineur, moyenne, majeure, critique.

Pour chacune des échelles, la fixation des différents intervalles doit être approuvée par les dirigeants puisque ces hypothèses de départ vont fortement influencer les résultats de la cartographie des risques.

[1] Gilbert Mareschal; Op.cit; p38.

L'échelle de la probabilité est la plus simple. En général, pour déterminer les intervalles on choisit une échelle entre 0 et 100%. Cependant pour certains risques, on peut choisir une échelle périodique, du type : se manifeste une fois tous les mois, ans, dix ans, etc.

Pour une activité industrielle, les défauts de fabrication ou les risques de panne peuvent être évalués par série : un tous les mille, dix mille objets, etc[1].

Tableau N°10 : Exemple d'échelles de probabilité

Échelle de probabilité	Rare	Possible	Probable	Quasi-certain
Score	1	2	3	4
Intervalle de probabilité	moins de 5 %	entre 5 et 20 %	entre 20 et 80 %	plus de 80 %
Occurrence par série	1 tous les millions	1 tous les mille	1 tous les cinquante	1 tous les cinq
Occurrence par période	1 fois par siècle	1 fois par an	1 fois par mois	1 fois par jour

Source : Mathieu Girème; Op.cit; p37.

L'échelle de la gravité de l'impact est plus subtile à évaluer dans le sens où elle doit être spécifique à chaque type de risque. La plupart des risques que l'entreprise encourt peut être monétairement quantifiée. C'est le cas d'un litige juridique, de charges induites par une réglementation ou une fiscalité défavorable, de la perte d'un client, des dégâts matériels suite à une catastrophe naturelle, d'un arrêt de la production. Dans le cas d'une cartographie groupe, il est plus judicieux de transposer les montants des dommages de chaque filiale en termes relatifs, par exemple en pourcentage du chiffre d'affaires, ou d'un autre indicateur plus approprié. Cela permet de faciliter la comparaison d'un risque et de son impact réel auprès d'une filiale par rapport aux autres entités du groupe. Pour les risques dont il est difficile d'évaluer monétairement l'impact, il faut alors déterminer des critères qualitatifs pour fixer les intervalles. Ainsi, pour un risque d'image et éventuellement pour un risque environnemental, il faut évaluer la répercussion médiatique de ce risque. Pour un risque de sécurité humaine, il faut fixer différents degrés d'incapacité d'un employé. Le risque de climat social, difficile à cerner, peut être appréhendé par différent indicateurs : sondage en interne, taux d'absentéisme, de turn-over, etc[2].

Tableau N°11 : Exemple d'échelles de gravité

Échelle de gravité	Faible	Modérée	Élevée	Critique
Score	1	2	3	4
Dépenses supplémentaires ou pertes de recettes	X euros ou X % de CA, de charges ou de RN	X euros ou X % de CA, de charges ou de RN	X euros ou X % de CA, de charges ou de RN	X euros ou X % de CA, de charges ou de RN
Poursuites judiciaires / contentieux	Entente à l'amiable	Saisine du tribunal	Condamnation au civil	Condamnation au pénal
Détérioration de l'image du Groupe	Limité à quelques personnes	Impact chez un ou plusieurs clients / fournisseurs	Impact dans la presse locale	Impact dans les médias nationaux / internationaux
Impact physique	Alerte sans arrêt de travail	Blessure avec arrêt de travail	Invalidité permanente d'un employé	Décès d'un employé ou d'un tiers
Impact efficacité / qualité, impact sur la qualité des données dans le SI	Altération légère de la qualité	Altération visible de la qualité	Interruption momentanée du service	Interruption prolongée du service

Source : Mathieu Girème; Op.cit; p38

[1] Gilbert Mareschal; Op.cit; p37.
[2] Idem ; p38.

L'échelle de criticité est le résultat de la cotation du risque sur les deux échelles précédentes. Elle est visuellement représentée par quatre couleurs dont les nuances tournent autour du vert, jaune et rouge sur la cartographie des risques. Pour chaque couleur, on peut attribuer une liste d'actions à prendre par défaut[1].

Tableau N°12: Exemple d'échelle de criticité

Échelle de criticité	Couleur	Description de la criticité
Risque mineur	Verte	Le risque est insignifiant et se situe très en dessous du seuil d'appétence.
Risque modéré	Jaune	Le risque a des conséquences qui demeurent tolérables, il faut néanmoins le surveiller.
Risque moyen	Orange	Le risque est mal ressenti par l'entreprise, les conséquences sont graves. Le risque doit absolument et rapidement être traité.
Risque majeur	Rouge	Le risque peut mettre jusqu'à la pérennité de l'entreprise en jeu. Dans tous les cas, l'entreprise est affectée durablement.

Source : Mathieu Girème; Op.cit; p39.

Comme nous venons de le décentrer, la connaissance des paramètres d'évaluation des risques mène à l'édification de la cartographie des risques et autorise leur hiérarchisation. En fait, il existe de nombreuses méthodes pour présenter les résultats de l'évaluation des risques, ces méthodes peuvent prendre la forme de cartographie des risques et de présentations numériques.

➲ ***L'hiérarchisation et la représentation graphique : la cartographie de risques***

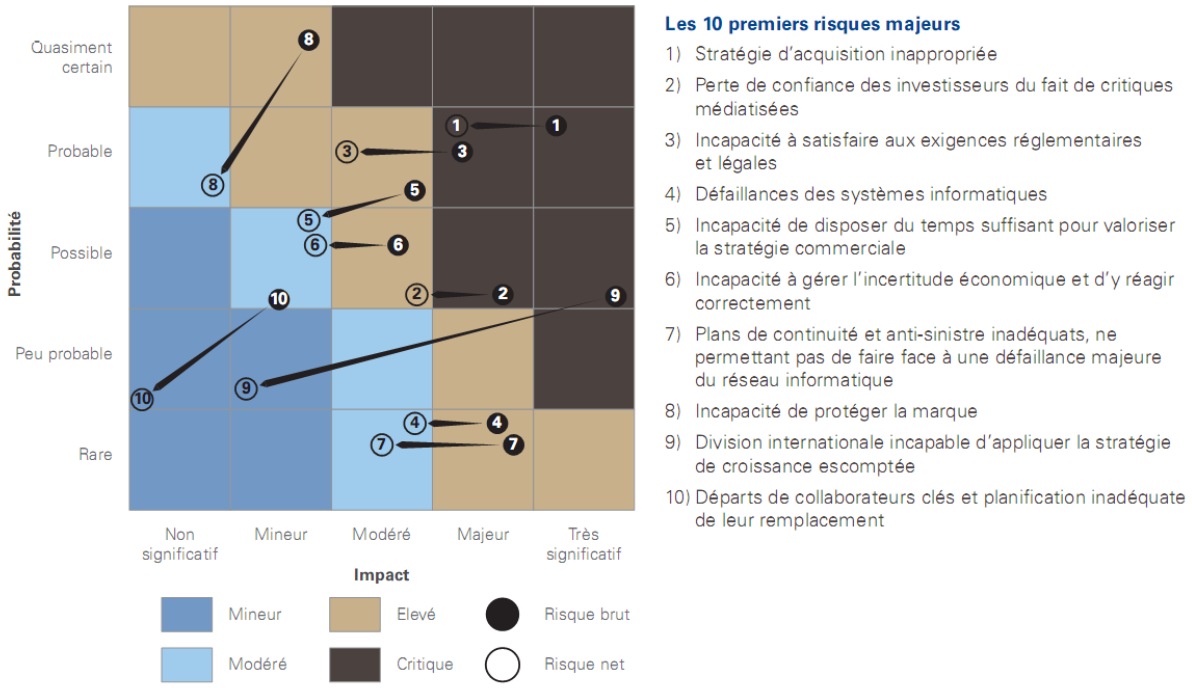
Rappelons qu'une cartographie des risques est une présentation graphique de la probabilité d'occurrence et l'impact d'un risque ou plusieurs risques. Les risques sont représentés de manière à identifier les risques les plus significatifs et les moins significatifs.

Ainsi, une cartographie des risques peut représenter le risque avant son traitement, pendant son traitement (évaluation de l'efficacité du traitement) et après son traitement.

Visuellement, il est possible de représenter le risque brut et le risque net sur la cartographie des risques. Ce type de cartographie est très intéressant puisqu'il permet d'évaluer l'efficacité de management du risque. En effet, l'inclinaison de la flèche entre le risque brut et le risque net renseigne à la fois sur la variation de la gravité et de la probabilité d'un risque. On peut également imaginer une cartographie des objectifs de management du risque qui contiendrait les risques résiduels majeurs et les niveaux de risque cible décidés par les dirigeants.

[1] Gilbert Mareschal; Op.cit; p 39.

Figure N°31 : Exemple de superposition de cartographie des risques nets et bruts[1*]



Sources : ACI & KPMG; Outil 7 : Exemple de cartographie des risques; Juin 2006; p1.

Pour décider des actions à prendre sur les risques résiduels, se référer à l'échelle de criticité peut suffire. Ainsi, le management peut estimer que tout risque dont la criticité est moyenne demeure intolérable et il faut alors décider des actions supplémentaires pour la diminuer.

Une autre analyse, qui nécessite de resituer les risques et celle proposée dans une des présentations de l'AFAI. Cette bonne pratique permet de répartir les contrôles effectués pour réduire les risques en quatre groupes[2] :

- Pour les risques inhérents forts, dont le risque résiduel est toujours fort, les contrôles ne sont pas assez efficaces, il faut les renforcer.

- Pour les risques inhérents forts dont le risque résiduel est faible, les contrôles sont satisfaisants et bien adaptés. Toutefois, étant donné le risque inhérent encouru, il faut s'assurer de l'application systématique du contrôle.

- Pour les risques inhérents faibles dont le risque résiduel est fort, ils ne sont a priori pas menaçants. Cependant, leur répétition et leur manque de surveillance peut à terme peser sur les activités de l'entreprise. Il faut donc surveiller le nombre de manifestation du risque.

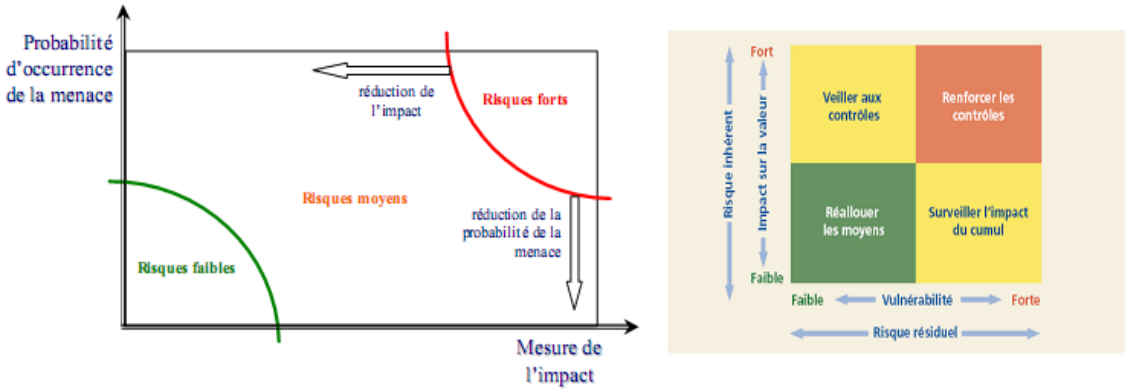
- Enfin les contrôles qui surveillent les risques inhérents faibles et dont le risque résiduel est faible sont peut-être trop nombreux. Il est peut être judicieux d'alléger les contrôles sur ces risques pour réallouer des moyens humains et matériels sur d'autres risques moins bien maîtrisés.

[1] Audit Committee Institut & KPMG Audit; Outil 7 : Exemple de cartographie des risques; Juin 2006; www.audit-committee-institute.fr; p1.

[*] La longueur des flèches est proportionnelle à l'efficacité des contrôles actuellement en place.

[2] Gina Gullà-Ménez en collaboration avec AFAI; Cartographie des risques informatiques : exemples, méthodes et outils ; Conférence présentée par le directeur de l'Audit des Processus et des Projets SI; Sanofi-Aventis & Vincent Manière ; Publiée par Association Française de l'Audit Informatique; 8 avril 2010.

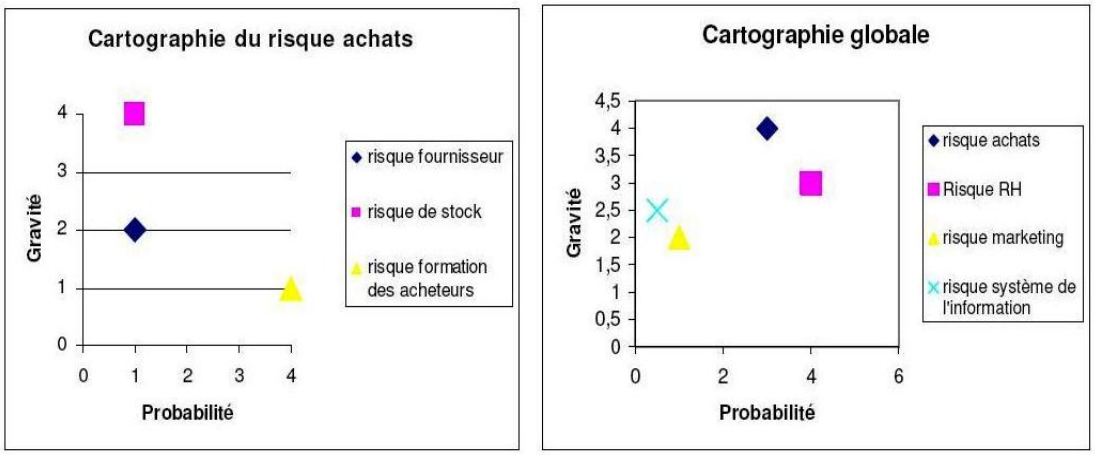
Figure N°32: Actions à prendre lors de l'analyse du risque résiduel



Source : Gina Gullà-Ménez en collaboration avec AFAI; Op.cit; p22.

En outre, en peut présenter les deux types de cartographies des risques, globale et thématique comme suit :

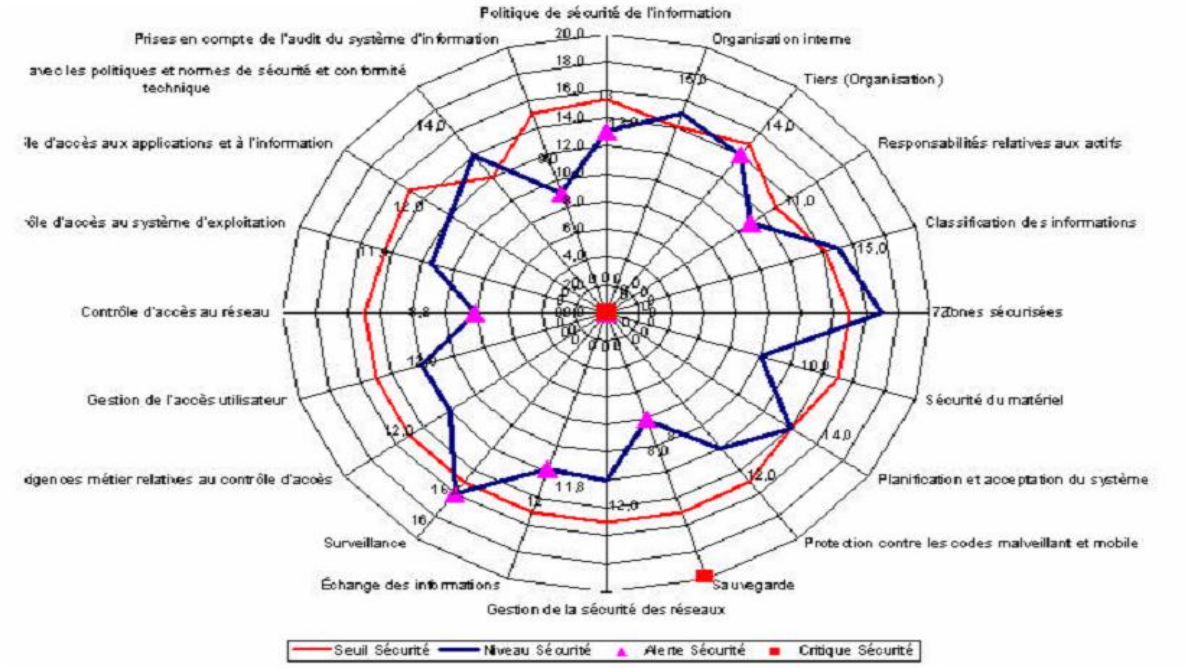
Figure N°33 : Exemples de la cartographie des risques globale et des risques d'achats



Source : Gina Gullà-Ménez en collaboration avec AFAI; Op.cit; p23.

Par ailleurs, parmi les présentations de la cartographie des risques, on peut citer le mode de radar ou toile d'araignée, comme ci figuré ci-dessous :

Figure N°34 : Exemples de la cartographie des risques en mode rosace



Source : Gina Gullà-Ménez en collaboration avec AFAI; Op.cit; p24.

➲ ***L'actualisation de la cartographie des risques***[1]

La cartographie des risques est une photographie de la situation à un instant donné, elle doit donc être actualisée afin de conserver la vision la plus appropriée, car le profil risque de l'entité est en perpétuel changement, et influencé par un certain nombre de facteurs, notamment :

- Les évolutions technologiques, réglementaires, et du marché ;

- Les nouveaux canaux de distribution ;

- Les modifications apportées en termes d'organisation et de système ;

- Les plan d'actions mis en place (actions correctives ponctuelles, procédures de contrôle récurrentes, transfert du risques…etc.).

L'actualisation de la cartographie permettra alors aux responsables d'observer l'impact de ces facteurs, de réajuster les plans d'actions déjà mis en place, et d'en définir de nouveaux.

En outre, La périodicité de l'auto-évaluation ne doit toute fois pas mener les participant à renouveler les mêmes constats à cause d'une périodicité fréquente, ni d'avoir une « photographie » périmée de la situation des risques à cause d'une périodicité longue. Une auto-évaluation approfondie tous les ans voir tous les deux ans permettra d'actualiser la vision des risques.

[1] IFACI, PwC et Landwell; COSO-II Report; Op.cit ; p 221.

3. Traitement des risques, surveillance et revue du processus Risk management

Après l'appréciation des risques, il est question de répondre auquel action à mettre en œuvre. Les différentes solutions possibles sont : l'évitement, la réduction, le partage et l'acceptation des risques. Le choix de tel traitement doit porter sur une solution ramenant les risques résiduels en deçà du seuil de tolérance souhaité par la direction général de l'organisation.

3.1. Traitement des risques

Une fois les risques identifiés et évalués, le management détermine quels traitements appliquer à chacun de ces risques. Le traitement du risque implique le choix et la mise en œuvre d'une ou de plusieurs options de modification des risques. Une fois mis en œuvre, les traitements engendrent ou modifient les moyens de maîtrise du risque.

Il existe quatre catégories de traitement de risque[1]:

- L'évitement : Cesser les activités à l'origine du risque. L'évitement du risque peut aussi bien avoir pour conséquence d'interrompre une ligne de produits, de ralentir l'expansion prévue sur un nouveau marché géographique que de vendre un département.
- La réduction : Prendre des mesures afin de réduire la probabilité d'occurrence ou l'impact du risque ou les deux à la fois. Il s'agit habituellement d'une multitude de décisions prises quotidiennement.
- Le partage: Diminuer la probabilité ou l'impact d'un risque en transférant ou en partageant le risque. Parmi les techniques courantes, citons l'achat de produits d'assurance, les opérations de couverture ou l'externalisation d'une activité.
- L'acceptation: Ne prendre aucune mesure pour modifier la probabilité d'occurrence du risque et son impact.

L'évitement suggère qu'aucune des réponses identifiées n'ait permis de réduire l'impact et la probabilité d'occurrence à des niveaux acceptables.

La réduction et le partage ramènent le risque résiduel à un niveau correspondant à la tolérance au risque, et l'acceptation laisse à penser que le risque inhérent se situe déjà dans la fourchette de tolérance au risque.

Pour de nombreux risques, les traitements appropriés sont évidents et bien acceptés. Par exemple, s'agissant du risque de panne informatique, une des options courantes est la mise en œuvre d'un plan de continuité d'activité. Pour d'autres risques en revanche, les options peuvent ne pas être aussi évidentes et nécessiteront une investigation et une analyse approfondie. Par exemple, parmi les réponses possibles pour limiter l'impact des activités de la concurrence sur la valeur d'une marque il peut être nécessaire de réaliser une étude de marché.

Le choix de traitement adéquats nécessite la prise en compte de facteurs tels que:

- L'effet des traitements potentiels sur la probabilité d'occurrence et l'impact des risques, et l'identification de ceux permettant de respecter la tolérance au risque de l'organisation.
- Le rapport coût/bénéfice des traitements potentiels.
- Les opportunités éventuelles, au-delà de la gestion du risque en question, permettant de contribuer à la réalisation des objectifs de l'organisation.

Pour les risques majeurs, les options potentielles seront déterminées sur la base d'un éventail de solutions possibles afin de procéder à un choix sur la base d'une analyse

[1] IFACI, PwC et Landwell; COSO-II Report; Op.cit ; p 84.

approfondie, que ce choix concerne la mise en œuvre d'un traitement ou l'adoption du « statu quo »

3.1.1. Évaluation des traitements possibles[1]

L'analyse des risques inhérents et l'évaluation des traitements des risques ont pour objectifs de parvenir à ramener le niveau de risque résiduel en deçà du seuil de tolérance au risque de l'organisation. Souvent, plusieurs traitements seront nécessaires pour ramener le risque résiduel à des niveaux correspondant à ce seuil et parfois l'atteinte d'un résultat optimal nécessitera d'effectuer une combinaison de différents traitements. En revanche, il peut arriver que le traitement d'un risque constitue une réponse appropriée à un éventail d'autre risques et qu'il ne soit donc pas nécessaire de prendre des mesures de traitements complémentaire pour ces derniers.

a) Évaluation des conséquences sur la probabilité et l'impact des risques [2]

Lorsque les différents traitements sont évalués, leurs conséquences sur la probabilité d'occurrence et sur l'impact des risques doivent être prises en compte; un même traitement pouvant avoir des répercussions différentes sur la probabilité d'une part et sur l'impact d'autre part. Citons l'exemple d'une société dont le centre informatique est situé dans une région sujette aux orages et ayant élaboré un plan de continuité d'exploitation. Bien que ce plan n'ait aucun effet sur la probabilité des orages, il en limite l'impact lié à l'endommagement des bâtiments ou à l'incapacité du personnel à travailler. En revanche, le choix de déménager le centre informatique dans une autre région ne diminuera pas l'impact d'un éventuel orage mais en réduira la probabilité d'occurrence.

Dans le cadre de l'analyse des traitements, il est possible de prendre en compte des événements et tendances historiques ainsi que des scénarii futurs potentiels. Dans le cas où des solutions alternatives nécessitent d'être évaluées, on utilise généralement des unités de mesure identiques ou homogènes à celle utilisées pour la mesure de l'objectif correspondant.

b) Évaluation des coûts/bénéfices[3]

La mobilisation de ressources comporte systématiquement une contrepartie, aussi convient-il d'analyser les coûts, comparativement aux bénéfices attendus des différents traitements des risques possibles. Les coûts et les bénéfices du traitement du risque sont mesurés avec divers degrés de précision. En règle générale, il est plus facile de traiter l'aspect «coûts/bénéfices» de l'équation, qui peut souvent être quantifiés assez précisément. Tous les coûts directs et indirects associés au choix d'un traitement sont pris en compte lorsqu'ils peuvent être mesurés. Certaines organisations tiennent également compte des manques à gagner découlant de l'utilisation des ressources.

Néanmoins, dans certains cas, il peut s'avérer difficile de quantifier le coût du traitement d'un risque. Les difficultés de la quantification proviennent de l'estimation du temps et des efforts associés à un traitement spécifique, comme cela peut être le cas lorsque l'on cherche à exploiter la veille commerciale relative à l'évolution des préférences des clients, aux activités de la concurrence ou à d'autre informations générées en externes.

Les bénéfices attendus impliquent souvent une évaluation plus subjective. Par exemple, les bénéfices tirés de programmes de formation efficaces sont généralement visible, quoique difficile à quantifier. Dans de nombreux cas cependant, les bénéfices liés au traitement d'un risque peuvent être évalués au regard de ceux dégagés si l'objectif concerné est atteint.

[1] IFACI, PwC et Landwell; COSO-II Report; Op.cit ; p 85.
[2] IFACI, PwC et Landwell; COSO-II Report; Op.cit ; p 86.
[3] Idem; p 86

Lors de l'analyse du rapport coûts/bénéfices, l'examen des interactions entre certains risques permet la mise en commun des traitements de risques de type réduction et partage. Par exemple, lorsqu'un risque est couvert par le biais d'une assurance, il peut s'avérer bénéfique de regrouper les risques dont le traitement est identique, les prix étant habituellement réduits lorsque plusieurs types de risques sont assurés par le biais d'une seule police.

c) Opportunités identifiées lors du traitement des risques[1]

La direction identifie les événements potentiels susceptibles d'affecter, positivement ou négativement, la réalisation des objectifs de l'organisation. Les événement ayant un impact positif représentent des opportunités et sont à réintégrer aux processus de définition de la stratégie ou de fixation des objectifs.

De la même façon, des opportunités peuvent être identifiées lors du traitement des risques. L'examen des traitements apportés aux risques ne doit pas se limiter à la réduction des risques identifiés, mais doit également prendre en compte les opportunités nouvelles offertes à l'entité. Des solutions novatrices sont susceptibles d'être identifiées qui, même si elles font partie d'une des catégories de traitement des risques, peuvent être totalement nouvelles pour une organisation ou un secteur. Parfois, de telles opportunités surgissent lorsque les traitements existants ont atteint un niveau d'efficacité tel qu'une amélioration supplémentaire n'aurait qu'un effet marginal sur l'impact ou la probabilité du risque traité.

3.1.2. Traitements sélectionnés[2]

Une fois évaluées les différentes alternatives en matière de traitement d'un risque, le management décide de la façon dans il compte gérer ce risque, et sélectionne un traitement ou une combinaison de traitements destinés à ramener la probabilité et l'impact des risques en deçà de son seuil de tolérance. Il n'est pas nécessaire que la solution retenue implique de minimiser le niveau de risque résiduel dépasse le seuil de tolérance. Dans certains cas le seuil de tolérance concerné sera reconsidéré. En conséquence, l'équilibre entre risque peut impliquer un processus itératif.

L'évaluation des différents traitements possibles d'un risque inhérent doit prendre en compte les risques supplémentaires susceptibles de découler de chaque traitement. Ceci peut également induire un processus itératif dans lequel, avant de finaliser sa décision, la direction tient compte de ces risques supplémentaires et en particulier de ceux qui pourraient passer inaperçus au premier abord.

Une fois le traitement d'un risque sélectionné, il peut être nécessaire d'élaborer un plan de mise en œuvre. Un des points cruciaux de cette mise en œuvre est la détermination des activités de contrôle permettant d'assurer la mise en application de la réponse retenue.

La direction doit avoir conscience du fait qu'il subsistera toujours un certain niveau de risque résiduel, non seulement du fait que ses ressources disponibles pour traiter les risques sont limitées, mais également du fait des incertitudes à venir et des limites inhérentes à toute activité.

3.1.3. Portefeuille des risques[3]

Le management des risques doit être considéré à l'échelle de l'organisation ou de façon globale afin d'en avoir une vue d'ensemble. Généralement, le risque est tout d'abord analysé au niveau de chaque unité, service ou fonction, leurs responsables effectuant une évaluation

[1] IFACI, PwC et Landwell; COSO-II Report; Op.cit ; p 87.
[2] IFACI, PwC et Landwell; COSO-II Report; Op.cit ; p 88.
[3] Idem; p 89.

composite des risques reflétant le profil de risque résiduel de l'unité compte tenu de ses objectifs et de sa tolérance au risque.

Connaître le niveau d'exposition aux risques de chaque entité permet à la direction générale de l'organisation d'obtenir une vision globale des risques et de déterminer si le profil de risque résiduels de l'organisation correspond à son appétences pour le risque au regard de ses objectifs. Il est possible par exemple que les risques résiduels de ces différentes unités se situent en deçà de leurs seuils de tolérance, mais qu'une fois agrégés, ils dépassent l'appétence de l'organisation pour le risque. Le cas échéant, il peut être nécessaire d'apporter des traitements supplémentaires ou différents pour ramener les risques dans les limites de l'appétence de l'organisation pour le risque. En revanche, à l'échelle de l'organisation certains risques peuvent se compenser mutuellement, par exemple lorsque certaines unités de management ont une exposition au risque élevée alors qu'elle est moindre chez d'autre. In fine, le risque global peut correspondre à l'appétence de l'organisation pour le risque qui ne nécessite donc pas de traitement complémentaire.

Il existe plusieurs possibilités de présenter un portefeuille des risques, par exemple, en se focalisant sur les risques principaux ou sur des catégories d'événement transversaux eux unités ou bien sur un risque identifié à l'échelle de l'organisation. Cette vision globale ou transversale est obtenue en utilisant des outils de mesure tels que le «capital adapté au risque» (risk-adjusted capital) ou le «capital-risque» (capital et risk). Ces mesures composites sont particulièrement utiles pour la mesure des risques au regard des objectifs de rentabilité, de croissance ou d'autre mesure de la performance comme l'allocation du capital ou le capital disponible. Ce type d'évaluation sur le portefeuille des risques est susceptible de fournir des informations utiles à la direction pour réaffecter le capital entre unités ou modifier des orientations stratégiques.

Prenons l'exemple d'une organisation de production utilisant cette vue d'ensemble des risques relative à ses objectifs en matière de résultat d'exploitation. Dans ce cas, le management utilise des catégories d'événement communes pour identifier les risques auxquels ses unités sont exposées. Il établit ensuite un diagramme illustrant, par catégorie et par unités, la probabilité d'occurrence des risques en termes de fréquence à un horizon donné, et l'impact sur les résultats. Il obtient ainsi une vue composite, une vue d'ensemble, de son exposition au risque et permet à la direction et au conseil d'administration d'examiner sereinement la nature, la probabilité d'occurrence et l'importance relative des risques, ainsi que leur impact éventuel sur les résultats de l'organisation.

On peut citer également le cas d'une institution financière qui demande à ses unités de définir des objectifs, des seuils de tolérance et des mesures de performance, tous ces éléments devant être exprimés en termes de rendement du capital ajusté en fonction des risques encourus. Ces mesures chiffrées appliquées par toutes les unités permettent à la direction d'agréger les évaluations des risques et d'obtenir une vue d'ensemble des risques de l'institution. Elle peut donc examiner les risques auxquels les unités sont exposées par objectif, et déterminer si l'entité reste dans les limites de son appétence pour le risque.

Le fait d'examiner les risques dans leur ensemble permet de déterminer si ceux-ci sont en ligne avec l'appétence de l'organisation pour le risque. En outre, la direction peut réévaluer la nature et le type de risque qu'elle souhaite prendre. Lorsque le portefeuille des risques montre que certains risques sont largement inférieurs à l'appétence de l'organisation pour le risque, la direction peut alors éventuellement inciter les responsables d'unités à accepter davantage de risques dans des domaines ciblés, afin d'augmenter la croissance et le rendement de l'organisation.

3.2. Surveillance et revue de processus d'évaluation des risques

Il convient que la surveillance et la revue soient planifiées dans le processus de management du risque et s'accompagne d'un contrôle ou d'une surveillance régulière. Ce contrôle ou cette surveillance peuvent être périodiques ou ponctuels.

Les activités de contrôle sont constituées des normes et procédures, et son représentées par les actions que les individus réalisent directement ou par le biais d'applications technologiques dans le but d'assurer l'exécution des directives émises par le management en vue de maîtriser les risques.

Les activités de contrôle reposent habituellement sur deux éléments : des normes qui définissent ce qui doit être fait, et des procédures pour réaliser ces objectifs.

Parallèlement à l'évaluation des risques, le management doit déterminer et mettre en œuvre le plan d'action destiné à les maîtriser. Une fois déterminées, ces actions devront également servir à définir les opérations de contrôle qui seront mises en œuvre pour garantir leur exécution correcte et en temps voulu

Les activités de contrôle interne doivent être évaluées dans le contexte des directives données par le management visant à traiter les risques associés aux objectifs retenus pour chaque activité importante.

Il existe de nombreuses catégories d'activités de contrôle comme les contrôles préventifs, détectives, manuels, informatiques, et de management. En outre, les activités de contrôle peuvent être regroupées par objectifs de contrôle, comme garantir l'exhaustivité et l'exactitude du traitement des données par exemple.

Nous allons décrire quelques activités de contrôle qui s'insèrent parmi les nombreuses procédures couramment utilisées par les collaborateurs à différents niveaux de l'organisation. Elles ont pour but d'encourager l'adhésion aux plans d'action existants et de permettre aux entités d'évoluer vers l'atteinte de leurs objectifs. Ces procédures sont présentées afin d'illustrer l'étendue et la diversité des activités de contrôle, et non dans l'idée de suggérer une quelconque catégorisation[1] :

✓ **Revues du management:** le management effectue une revue de performance en comparant les réalisations au regard du budget, des prévisions, des périodes précédentes et de la concurrence. Les actions majeures comme les actions marketing, les améliorations du processus de production ou les programmes de réduction ou de maîtrise des coûts, font l'objet d'un suivi afin de mesurer l'atteinte des objectifs. La mise en œuvre des projets pour le développement de nouveaux produits, les joint-ventures ou les opérations de financement font également l'objet d'un suivi.

✓ **Supervision directe d'une activité ou d'une fonction:** les responsables de fonction ou d'activité revoient les rapports de performance. Dans une banque, le responsable des crédits à la consommation revoit les rapports par succursale, par région et par type de prêt. Il vérifie les rapports de synthèse et identifie les tendances et leurs répercussions sur les objectifs de performance et les statistiques économiques. En retour, les responsables de succursales reçoivent des données sur les nouveaux crédits ventilés par responsable crédit et secteur de clientèle. Les responsables de succursales portent également une attention particulière aux problématiques de conformité et revoient les rapports requis par les régulateurs sur les nouveaux dépôts supérieurs à certains seuils. Des rapprochements des flux de trésoreries quotidiens sont effectués, les positions nettes faisant l'objet d'un reporting centralisé pour les virements et les placements au jour le jour.

[1] IFACI, PwC et Landwell; COSO-II Report; Op.cit; p 96-97.

✓ **Traitement de l'information:** de nombreux contrôle sont effectués pour vérifier l'exactitude, l'exhaustivité et la validation de transaction. Les données saisies sont soumises à des vérifications ou à des rapprochements par rapport à des tables de contrôle. Par exemple, la commande d'un client n'est acceptée qu'après consultation du dossier client validé et du plafond de crédit. Les séquences numériques des transactions sont examinées et les exceptions sont suivie et signalées aux responsables. Le développement de nouveaux systèmes et la modification des systèmes existants sont contrôlés, de même que l'accès aux données, aux fichiers et aux programmes.

✓ **Contrôle physique:** la sécurité physique des équipements, des stocks, des valeurs, des liquidités et des autres actifs est assurée et ces biens sont inventoriés périodiquement, l'inventaire physique étant rapproché des montants comptabilisés.

✓ **Indicateurs de performance:** le fait de rapprocher différentes catégories de données (opérationnelles ou financières) et de faire l'analyse des liens existants entre elles, de poursuivre des actions d'investigation ou de mettre en œuvre des mesures correctives, constituent une activité de contrôle. Parmi ces indicateurs de performance on peut citer les taux rotation du personnel par unité. En analysant les résultats inattendus ou les tendances inhabituelles, la direction identifie les circonstances où l'incapacité à mettre en œuvre un processus clé susceptible de susceptible de réduire la probabilité d'atteinte des objectifs. La façon dont la direction utilise ces informations – soit pour prendre des décisions opérationnelles soit pour faire également un suivi des résultats imprévus dans le cadre des systèmes de reporting – détermine si l'analyse des indicateurs de performance répond uniquement à des objectifs opérationnels ou également à des objectifs de reporting.

✓ **Séparation des tâches:** les tâches sont divisées ou réparties entre différentes personnes, ce qui permet de réduire le risque d'erreur ou de fraude. Par exemple, les responsabilités concernant l'autorisation des transactions, leur enregistrement et le management de l'actif concerné sont séparées. Un responsable autorisant l'octroi de crédits ne peut être également en charge de la tenue des comptes clients ou de la réception des sommes perçues en liquide. De même, un commercial ne devrait pas pouvoir modifier le fichier des tarifs proposés aux clients ni les taux des commissions.

Il convient que les responsabilités de surveillance et de revue soient clairement définies. Il convient aussi que les processus de surveillance et de revue de l'organisme s'appliquent à tous les aspects du processus de management du risque afin de pouvoir [1]:

✓ s'assurer que les moyens de maîtrise sont efficaces et performants aussi bien dans leur conception que dans leur utilisation,

✓ obtenir des informations supplémentaires pour améliorer l'appréciation du risque,

✓ analyser et tirer les leçons des événements (y compris des incidents), des changements, des tendances, des succès et des échecs,

✓ détecter les changements dans le contexte interne et externe, y compris les changements concernant les critères de risque et le risque lui-même qui peuvent nécessiter une révision des traitements du risque et des priorités, et

✓ identifier les risques émergents.

L'avancement de la mise en œuvre des plans de traitement des risques constitue une mesure de la performance. Les résultats peuvent être intégrés au management global des performances de l'organisme, à leur mesurage et aux activités d'élaboration de rapports externes et internes.

[1] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit; p21.

Lorsque les aléas sont connus ou prévus, la cartographie actualisée des risques intervient pour supporter les décisions concernant la gestion des alertes. Selon le niveau d'alarme, une nouvelle itération du cycle de management des risques sera lancée (Bakir, 2003). Si l'événement est inconnu, il est alors identifie pour une prise en compte au cours des itérations futures.

Dans certains cas, le suivi des risques révèle un changement considérable du périmètre d'étude qui impliquera une relance de management des risques avec des objectifs raffines. Il s'agira, par exemple, de focaliser le processus de gestion sur une dimension particulière du périmètre d'étude comme par exemple le cout, la qualité ou le délai en gestion de projet. C'est souvent le cas dans la situation de crise.

Il faut noter que cette étape de management des risques collecte l'information indispensable a la conduite du système, au retour d'expérience et a l'amélioration du processus de management des risques.

Il convient que les résultats de la surveillance et de la revue soient enregistrés, fassent l'objet de rapports internes et externes selon les besoins, et servent de données à la revue du cadre organisationnel de management du risque.

- **Enregistrement du processus de management du risque**[1]

Il convient que les activités de management du risque puissent être tracées. Dans le processus de management du risque, les enregistrements fournissent la base de l'amélioration des méthodes et des outils ainsi que du processus dans son ensemble.

Il convient que les décisions relatives à la création des enregistrements prennent en compte

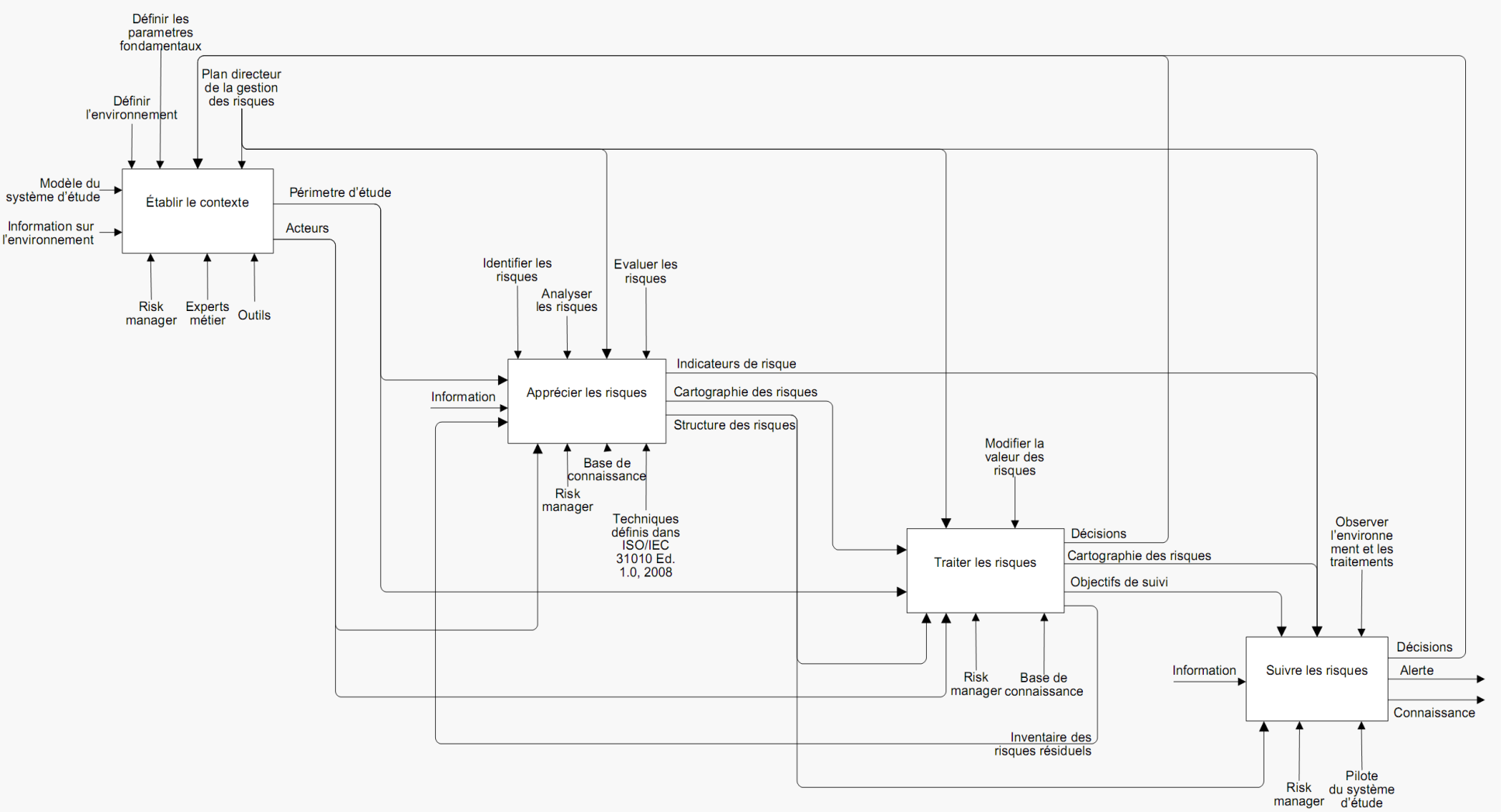
- les besoins de l'organisme en matière d'acquisition continue de connaissances ;
- les avantages de la réutilisation d'informations pour répondre à des objectifs de management ;
- les coûts et le travail liés à la création et à la maintenance des enregistrements ;
- les nécessités légales, réglementaires et opérationnelles d'effectuer des enregistrements ;
- la méthode d'accès, la facilité de consultation et les moyens de stockage ;
- la période de conservation ;
- le caractère sensible des informations.

3.3. Synthèse

Les interdépendances entre les différentes phases du processus de management du risque sont schématisées dans la figure ci-après :

[1] ISO/DIS 31000; Risk management-Principles and guidelines; Op.cit; p 21.

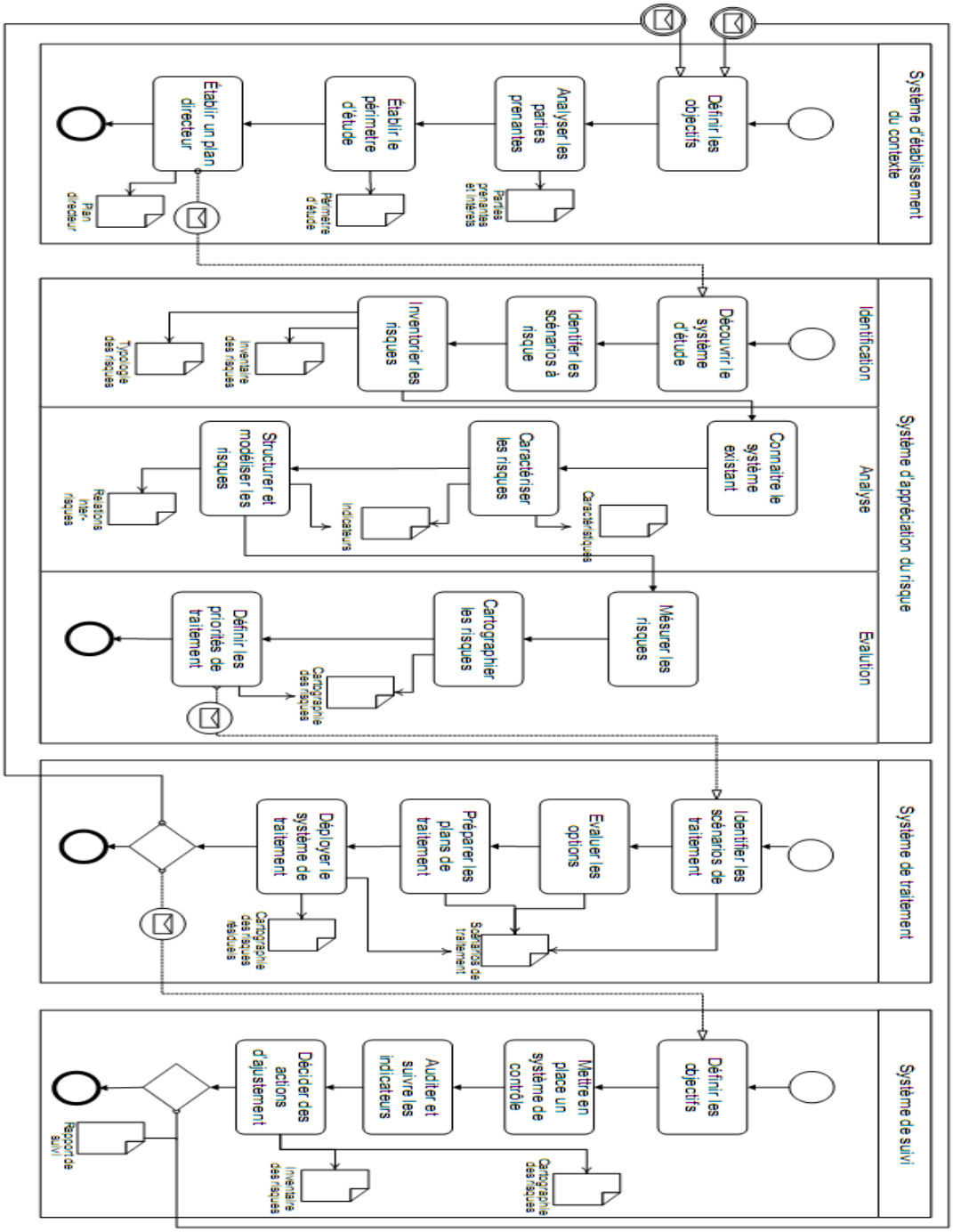
Figure N°35 : Le processus de management du risque selon le modèle SADT/IDEFO



Sources : Amadou SIENOU; Proposition d'un cadre méthodologique pour le management intégré des risques et des processus d'entreprise; Op.cit ; p 82.

Le modèle structurel proposé par Amadou SIENOU, met en évidence l'agencement logique et temporel des activités dans une finalité de réalisation des objectifs de management du risque. Les étapes « établir le contexte », « apprécier », « traiter » et « suivre » se comportent chacune comme un processus délimité par un début et une fin. La synchronisation interprocessus est assurée par des échanges de messages auxquels sont associés les résultats de l'effort de modélisation, comme suit :

Figure N°36 : Le processus de management du risque selon le modèle fonctionnel BPMN

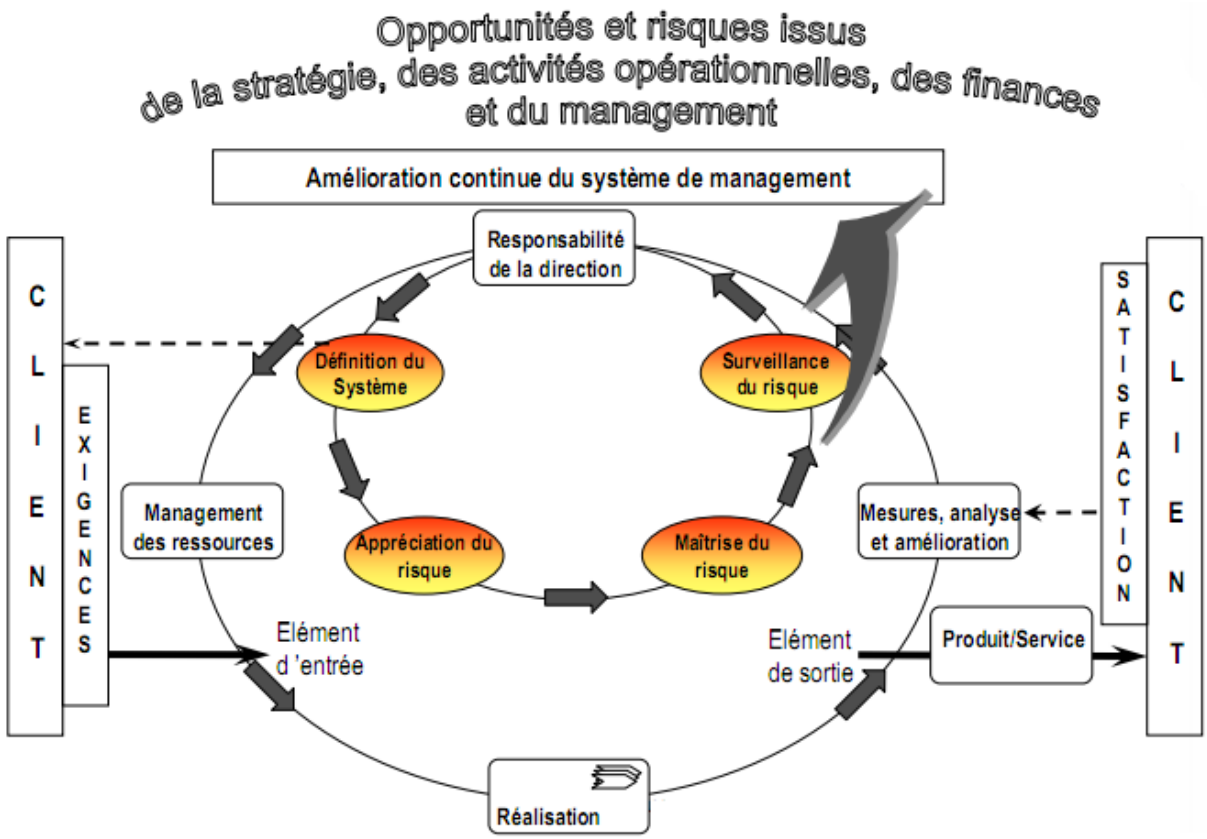


Sources : Amadou SIENOU; Op.cit ; p 83.

Nous avons mené à la présente section une analyse du processus risque management, cette analyse nous a permis de affirmer que le management du risque en entreprise est une approche systémique qui recherche l'amélioration des décisions en milieu incertain pour maitriser la préservation de la valeur d'entreprise.

C'est une démarche qui permet d'établir un équilibre entre les attentes dans une plage de variations acceptables de la valeur, et d'assurer un déploiement efficace des ressources. Le management du risque favorise une bonne appréciation de la richesse et de la finesse des relations entre la valeur et la préservation de la valeur[1].

Figure N°37 : L'intégration du processus de management du risque aux processus d'organisation



Source : ON 49000 La gestion du risque - Ligne directrices ; Op.cit; p62.

Le management des processus et le management du risque s'articulent donc tous deux autour de la valeur : l'un pour la créer et l'autre pour la préserver. Ces deux approches de management semblent nativement être indépendantes l'une de l'autre, et former deux mondes complémentaires. Mais il faut noter une préoccupation récente initiée par le monde industriel qui tend à les combiner, et à travailler sur des intersections, pour des applications comme la conformité règlementaire ou la planification de la continuité des activités.

[1] ON 49000: La gestion du risque pour les organisations et les systèmes - Ligne directrices ; Op.cit ; p 62.

Section 2 : Les méthodes et les techniques d'analyse et d'évaluation des risques

L'évaluation des risques peut être réalisée à divers degrés de profondeur et de détail et par de nombreuses méthodes, de la plus simple à la plus complexe. Il convient que la forme de l'évaluation et son résultat soient cohérents avec les critères de risque développés dans le cadre de l'établissement du contexte. Dans cette partie seront détaillées les méthodes les plus usuelles et les plus pertinentes en matière d'analyse de risques pour mettre en avant leurs besoins et leurs finalités.

1. Sélection et classification des méthodes d'évaluation des risques

Dans ce qui suit, nous allons expliquer la manière dont les organisations peuvent sélectionner et classifier les techniques d'évaluation des risques appropriées pour une situation particulière.

De manière générale, il convient qu'une technique adaptée possède les caractéristiques suivantes [1]:

- Il convient qu'elle soit justifiée et adaptée à la situation ou à l'organisation considérée;
- Il convient que les résultats obtenus se présentent sous une forme permettant une meilleure compréhension de la nature des risques et de la manière dont ils peuvent être traités;
- Il convient qu'elle soit utilisée de telle sorte qu'elle soit traçable, reproductible et vérifiable.

1.1. Critères du choix d'une méthode d'analyse de risque [2]

Sur la base des critères que l'organisation peut choisir de mettre en œuvre d'une méthode plutôt qu'une autre dans l'étude d'un système donné, nous pouvons retenir l'essentiel de ces critères comme suit:

✓ **Domaine et objectifs de l'étude**: les objectifs de l'évaluation des risques auront un effet direct sur les techniques utilisées. Par exemple, s'il est entrepris une étude comparative entre différentes option, il peut être acceptable d'utiliser des modèles de conséquence moins détaillés pour les parties du système qui ne sont pas affectées par les différences d'option;

✓ **Les besoins des décideurs**: dans certains cas, un niveau de détail élevé est nécessaire pour prendre une bonne décision, alors que dans d'autre cas, une compréhension plus générale est suffisante;

✓ **La perception et le type de l'ensemble des risques en cours d'analyse**;

✓ **L'amplitude potentielle des conséquences**: il convient que la décision prise quant au niveau de profondeur de l'évaluation des risques reflète la perception initiale des conséquences (même s'il peut s'avérer nécessaire de la modifier après réalisation d'une évaluation préliminaire);

✓ **Le degré de compétence, ainsi que les besoins en ressources humaines et autre**: une méthode simple, correctement mise en œuvre, peut souvent donner de meilleurs résultats qu'une procédure plus sophistiquée d'application médiocre, si elle satisfait aux objectifs et au domaine d'application de l'évaluation.

✓ **Le retour d'expérience et la disponibilité des informations**. Certaines techniques nécessitent plus d'informations et de données que d'autres, selon les caractéristiques du problème à analyser, et la nature des informations disponibles;

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit. P 109
[2] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit. P 109-110.

✓ **La modification/mise à jour nécessaire de l'évaluation des risques.** Il est admis que l'évaluation puisse nécessiter des modifications/mises à jour future et qu'à cet égard, certaines techniques soient, plus que d'autre, susceptible d'être modifiées;

✓ Culture de la sûreté de fonctionnement de l'organisation et toutes exigences réglementaires et contractuelles.

1.2. Facteurs influençant le choix[1] :

Différents facteurs influencent le choix d'une approche de l'évaluation des risques, nous les citons comme suit:

1.2.1. Disponibilité des ressources

Les ressources et capacités pouvant avoir un impact sur le choix des techniques d'évaluation des risques comprennent:

• Les compétences, l'expérience, la capacité et les aptitudes de l'équipe d'évaluation des risques;

• Les contraintes liées au temps et aux autres ressources de l'organisation;

• Le budget disponible si des ressources externes sont requises.

1.2.2. Nature et degré d'incertitude

La nature et le degré d'incertitude exigent une bonne connaissance de la qualité, de la quantité et de l'intégrité des informations disponibles relatives au risque considéré. Il s'agit de savoir dans quelle mesure les informations suffisantes relatives au risque, à leurs sources et à leurs causes, ainsi que leurs conséquences sur l'atteinte des objectifs sont disponibles. L'incertitude peut provenir de la qualité médiocre des données ou de l'absence de données essentielles et fiables. A titre d'illustration, les méthodes utilisées pour rassembler des données peuvent changer, de même que la manière dont les organisations utilisent ces méthodes, ou l'organisation peut ne pas avoir de méthode particulière pour rassembler des données relatives au risque identifié.

L'incertitude peut également être inhérente au contexte externe et interne de l'organisation. Les données disponibles ne constituent pas toujours une base fiable de prédiction de l'avenir.

Pour les types uniques de risques, les données historiques peuvent ne pas être disponibles, ou celles qui le sont peuvent faire l'objet de différentes interprétations par différents acteurs. Cette évaluation des risques entreprise doit cerner le type et la nature de l'incertitude et apprécier les implications quant à la fiabilité des résultats de l'évaluation. Il convient de toujours communiquer ces éléments aux décideurs.

1.2.3. Complexité

Les risques peuvent être complexes par nature, par exemple, dans les systèmes complexes dont les risques doivent être évalués dans le cadre du système plutôt qu'en traitant chaque composant séparément et en ignorant les synergies. Dans d'autres cas, le traitement d'un seul risque peut avoir des implications ailleurs et avoir un impact sur d'autres activités. Les impacts importants et dépendances du risque doivent être compris pour s'assurer que de la gestion d'un seul risque ne découle pas une situation intolérable ailleurs. Il est essentiel de comprendre la complexité d'un seul risque ou d'un ensemble de risques d'une organisation pour choisir la méthode ou la technique adaptée à l'évaluation des risques.

[1]ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit. P110.

1.2.4. Application de l'évaluation des risques au cours du cycle de vie[1]

Il est possible de considérer que le cycle de vie de la plupart des activités, projets et produits commence au concept et à la définition initiale et se poursuit jusqu'à l'achèvement, qui peut inclure le déclassement et la mise au rebut du matériel.

Les risques peuvent être évalués à toutes les étapes du cycle de vie. D'une manière générale, ils le sont plusieurs fois à différents niveaux de détail, de manière à faciliter la prise de décision à chaque phase.

Les phases du cycle de vie répondent à différentes exigences et nécessitent d'appliquer différentes techniques. Par exemple, lors de la phase de conception et de définition, si une opportunité est identifiée, les risques peuvent être évalués pour décider de la poursuite ou de l'interruption.

Si plusieurs options sont disponibles, les risques peuvent être évalués pour mesurer d'autres concepts et déterminer plus facilement lequel offre le meilleur rapport entre les risques positifs et négatifs.

Lors de la phase de conception et de développement, l'évaluation des risques permet

• d'assurer que les risques liés au système sont tolérables,

• de participer au processus d'amélioration de la conception,

• de participer aux études de rentabilité,

• d'identifier les risques ayant un impact sur les phases suivantes du cycle de vie.

Au fur et à mesure du déroulement de l'activité, il est possible d'évaluer les risques pour apporter des informations facilitant les procédures de développement pour les conditions normales et d'urgence.

1.3. Classification des méthodes d'analyse de risque

Actuellement les approches d'évaluation des risques se diversifient, se sophistiquent. Les techniques d'évaluation de risque peuvent être classées de différentes manières afin de faciliter la compréhension de leurs forces et faiblesses relative. En fait, il n'y a pas de solution universelle et les entreprises qui implantent une approche avancée de Risk management sont conduites à mixer plusieurs méthodes pour cartographier l'ensemble de leurs risques.

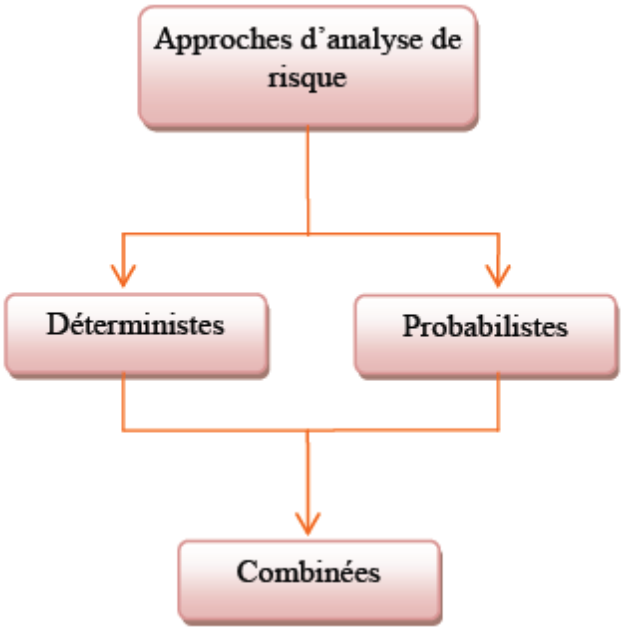
Nous recensons, selon plusieurs critères qui peuvent se croiser, des approches déterministes et probabilistes, des approches quantitatives et qualitatives.

1.3.1. Approches déterministes et probabilistes:

D'une manière générale, l'évaluation du risque est probabiliste. Toute analyse de risques qui se veut aussi exhaustive que possible ne peut se priver d'éléments d'incertitude, qui plus est, la notion d'acceptabilité a également facilité la promotion de cette démarche. Toutefois, s'agissant de la sûreté de fonctionnement d'une installation ou d'un système présentant des risques industriels, l'approche déterministe reste l'approche privilégiée[2].

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; P110.
[2] Marc Fumey; Op.cit. P81

Figure N38°: Approche d'analyse de risque



Source: Mohamed –Habib Mazouni; op.cit. p 46.

a) Approche déterministe[1]

L'approche déterministe a généralement été adoptée dans les domaines à haut risque tels que nucléaire, militaire, transports guidés, où le moindre risque significatifs est traqué et réduit à la source. Elle consiste à recenser les événements pouvant conduire à un scénario d'accident en recherchant le pire cas possible (The Worst Case) et en affectant une gravité extrême à ses conséquences potentielles. Par conséquent, les sous-systèmes critiques (systèmes de sauvegarde, de protection et de prévention) sont dimensionnés pour éviter toute défaillance dangereuse et organisés rigoureusement selon une stratégie de défense en profondeur.

Du fait de l'absence d'éléments d'incertitude, la qualité de cette approche est conditionnée par l'état des connaissances et ne peut donc satisfaire l'analyse des risques émergents et liés à des situations nouvelles, complexes et non entièrement maîtrisées.

b) Approche probabiliste[2]

L'approche probabiliste repose sur l'estimation de la probabilité relative à l'occurrence d'événements faisant partie du processus de matérialisation d'un scénario d'accident donné. Dans ce sens, la maîtrise des risques consiste à démontrer que la probabilité de survenue est maintenue à des valeurs acceptables, si besoin est par ma mise en place de mesures destinées à les réduire.

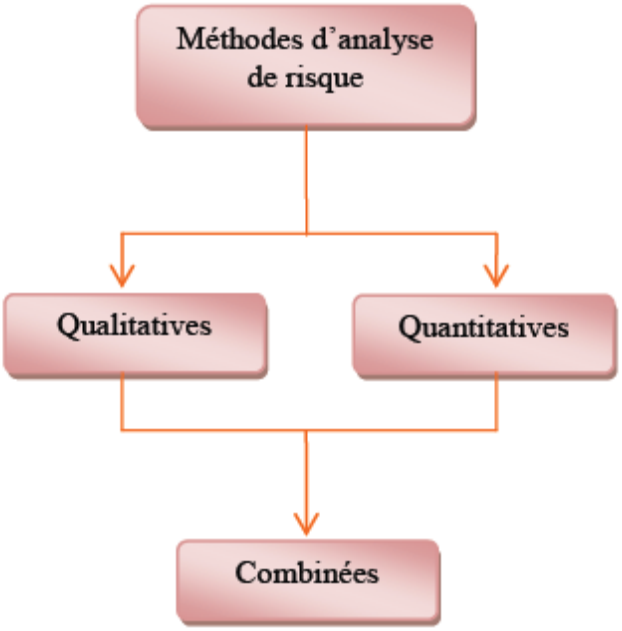
L'évaluation des risques repose alors sur une analyse probabiliste des indices de probabilités et de conséquence. Il s'agit d'une approche complémentaire qui permet d'analyser le dispositif de défense en profondeur décidé à l'issue d'une approche purement déterministe, ceci a été largement développée sur l'appellation Evaluation Probabilité de Risques ou EPR dans le domaine nucléaire, du pétrole et de la chimie, ou les techniques probabilistes viennent appuyer l'approche déterministe.

[1] Mohamed –Habib Mazouni; op.cit. p 46
[2] Mohamed –Habib Mazouni; op.cit. p 46

1.3.2. Méthodes qualitatives vs méthodes quantitative

Les approches d'évaluation des risques sont généralement constituées d'une combinaison de techniques qualitatives et quantitatives, selon le schéma suivant:

Figure N°39 : Typologie des méthodes d'analyse de risque



Source: Mohamed –Habib Mazouni; *op.cit*. p 47.

a) Méthodes quantitatives [1]

Les techniques quantitatives donnent en règle générale des résultats plus précis et sont utilisées pour compléter les techniques qualitatives sur les activités les plus complexes.

Les analyses quantitatives sont supportées par des outils mathématiques ayant pour but d'évaluer la sûreté de fonctionnement et entre autres la sécurité. Cette évaluation peut se faire par des calculs de probabilités (par exemple lors de l'estimation quantitative de la probabilité d'occurrence d'un événement redouté) ou bien par recours aux modèles différentiels probabiliste tels que les chaines de Markov, les réseaux de pétri, les automates d'états finis, etc.

Les analyses quantitatives ont de nombreux avantages car elles permettent:

- D'évaluer la probabilité des composantes de la sûreté de fonctionnement.
- De fixer des objectifs de sécurité.
- De juger de l'acceptabilité des risques en intégrant les notions de périodicité des contrôles, la durée des situations dangereuses, la nature d'exposition, etc.
- D'apporter une aide précieuse pour mieux juger du bien d'améliorer la sécurité.
- De hiérarchiser les risques.
- De comparer et ensuite ordonner les actions à entreprendre en engageant d'abord celles permettant de réduire significativement les risques.
- De chercher de meilleure coordination et concertation en matière de sécurité entre différents opérateurs (sous système interagissant) ou équipe (exploitation, maintenance, etc.).

[1]Mohamed –Habib Mazouni. Op.cit. P47.

Quoique l'utilité des méthodes quantitative soit indiscutable, ces dernières présentent tout de même un certain investissement en temps, en efforts et également en moyen (logiciels, matériels, financiers, etc). Il peut s'avérer que cet investissement soit disproportionné par rapport à l'utilisé des résultats attendus, le cas échéant l'analyse quantitative est court-circuitée pour laisser la place aux approximations qualitatives (statistiques, retour d'expérience, jugement d'expert, etc.).

Un point très important mérite d'être clarifié, c'est que les résultats de l'analyse quantitative ne sont pas des mesures absolues, mais plutôt des moyens indispensables d'aide au choix des actions pour la maîtrise des risques. Nous citons par exemple l'évaluation par des techniques floues/possibilistes de la subjectivité des experts humains, ou la priorisation de certaines actions de maîtrise par rapport à d'autre par une analyse de type coût/bénéfices.

b) Méthodes qualitatives[1]

Le management utilise fréquemment des techniques d'évaluation qualitatives lorsque les risques ne se prêtent pas à la quantification ou lorsqu'il ne dispose pas des données nécessaires à une évaluation quantitative ou encore lorsque la collecte et l'analyse de ces données n'est pas rentable au regarde du bénéfice attendu.

Une méthode qualitative consiste à évaluer le risque en structurant la connaissance recueillie auprès des «expert». Elle est dite subjective dans la mesure où elle s'appuie sur des opinions exprimées pour en tirer une évaluation de risque.

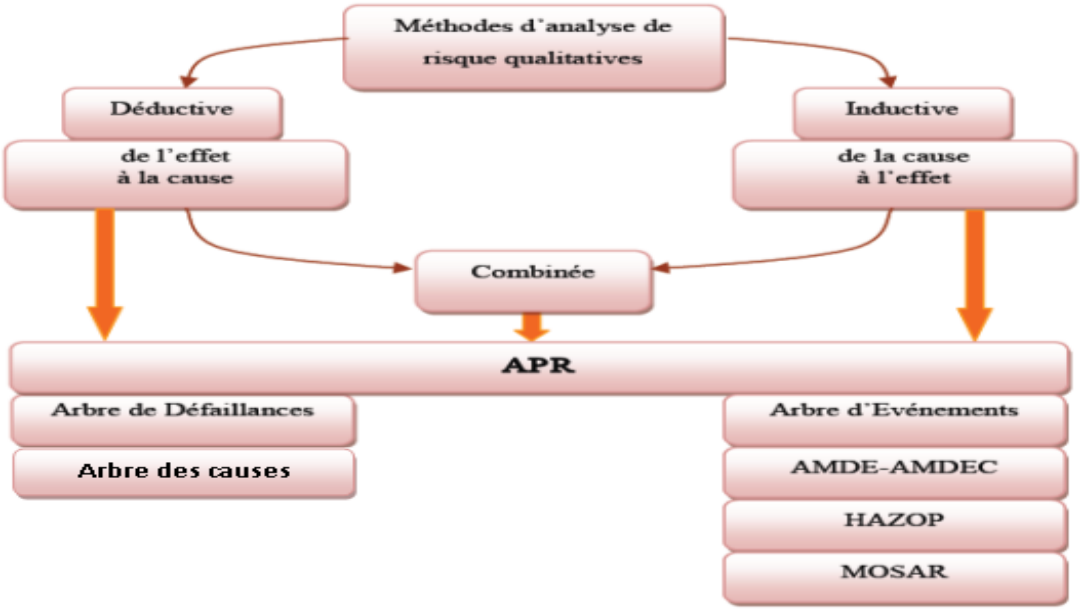
L'APR, l'AMDEC, l'Arbre de Défaillances ou l'Arbre d'Evénements restent des méthodes qualitatives même si certaines mènent parfois aux estimations de fréquences d'occurrence avant la classification des risques.

L'application des méthodes d'analyse de risque qualitatives fait systématiquement appel aux raisonnements par induction et par déduction.

La plupart des méthodes revêtent un caractère inductif dans une optique de recherche allant des causes aux conséquences éventuelles. En contrepartie, il existe quelques méthodes déductives qui ont pour but de chercher les combinaisons de causes conduisant à des évènements redoutés.

[1]Mohamed –Habib Mazouni. Op.cit. P47.

Figure N°40 : classification des principales méthodes d'analyse de risque qualitative



Source: Mohamed –Habib Mazouni. Op.cit. P48.

Une méthode est dite déductive si elle cherche les causes d'un événement redouté. Le concept de déduction renvoie généralement à une démarche selon laquelle on se base plutôt sur la connaissance préalable des effets et on cherche justement à remonter causalement jusqu'aux origines de leur apparition. Les plus connues et les plus utilisées sont les méthodes dites de l'arbre des causes et de l'arbre des défaillances.

Contrairement à la méthode déductive, une méthode est dite inductive si elle consiste à déterminer les scénarios d'événement non souhaité qui en résultent et/ou l'ensemble de ses conséquences possibles. Ce concept d'induction renvoie à une démarche selon laquelle on part de la connaissance d'une cause et on essaye de déterminer les effets qu'elle susceptible de provoquer. Les méthodes les plus utilisées et que nous les présenterons après sont l'HAZOP, MOSAR, l'AMDE-AMDEC et l'arbre des événements[1].

2. Panorama des méthodes

Le panorama des méthodes fait l'objet de nombreuses parutions scientifiques et pratiques. Nous allons présenter dans cet élément un échantillonnage de l'ensemble de ces méthodes d'analyse de risque.

2.1. Les méthodes quantitatives

Les techniques quantitatives peuvent être utilisées lorsqu'il existe suffisamment d'information permettant d'estimer la probabilité d'occurrence ou l'impact d'un risque sur la base d'évaluation par intervalle ou ratio. Les méthodes quantitatives intègrent des techniques statistiques, non statistiques et de benchmarking. Il est important de tenir compte, dans le cadre des évaluations quantitatives, da la disponibilité de données fiables, provenant de sources aussi bien internes qu'externes. Une des principales difficultés de ces techniques est d'obtenir suffisamment de données valides. Nous citerons ci-après quelques méthodes pertinentes dans le cadre d'évaluation quantitative :

[1] Mohamed –Habib Mazouni. Op.cit. P48.

2.1.1. Analyse de Markov[1]

Le processus d'analyse de Markov est une technique quantitative qui peut être discrète (utilisant des probabilités de passage d'un état à l'autre) ou continue (utilisant les vitesses de passage d'un état à l'autre). Cette analyse est utilisée lorsque l'état futur d'un système dépend uniquement de son état présent. Elle est en général utilisée pour analyser les systèmes réparables comportant plusieurs états, une analyse par bloc de fiabilité étant inappropriée à l'analyse pertinente du système. La méthode peut être étendue à des systèmes plus complexes grâce à des chaînes de Markov d'ordre supérieur et est uniquement limitée par le modèle, les calculs mathématiques et les hypothèses.

La technique d'analyse de Markov peut être utilisée sur différentes structures de système, avec ou sans réparation, notamment:

- les composants indépendants en parallèle;
- les composants indépendants en série;
- les systèmes de partage de charge;
- les systèmes autonomes, y compris les cas dans lesquels une défaillance de communication peut se produire;
- les systèmes dégradés.

La technique d'analyse de Markov peut également permettre de calculer la disponibilité notamment en tenant compte des composants de rechange destinés à la réparation.

Les entrées essentielles à une analyse de Markov sont les suivantes:

- liste de différents états dans lesquels peut se trouver le système, le sous-système ou le composant (complètement opérationnel, partiellement opérationnel (c'est-à-dire à l'état dégradé), état défaillant, par exemple);
- une bonne compréhension des transitions possibles dont la modélisation est nécessaire. Par exemple, la dégradation d'un pneu de voiture doit tenir compte de l'état de la roue de secours, et donc de la fréquence d'inspection;
- la vitesse de passage d'un état à l'autre est en général représentée par une probabilité de changement d'état pour les événements discrets, ou par le taux de défaillance (λ) et/ou la fréquence de réparation (μ) pour les événements continus.

La technique d'analyse de Markov tourne autour du concept «d'état» (disponible et en panne, par exemple), le passage entre chacun d'eux dans le temps reposant sur une probabilité constante de modification. Une matrice de probabilité de transition stochastique permet de décrire la transition entre chacun de ces états afin de calculer les différents résultats.

Pour illustrer la technique d'analyse de Markov, soit un système complexe ne pouvant faire l'objet que de trois états: fonctionnement, dégradé et en panne, chacun d'eux étant respectivement défini comme les états S1, S2 et S3. Chaque jour, le système évolue dans l'un de ces trois états. Le Tableau B.3 illustre la probabilité de trouver demain le système à l'état S*i*, où *i* peut être 1, 2 ou 3.

1 ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p164.

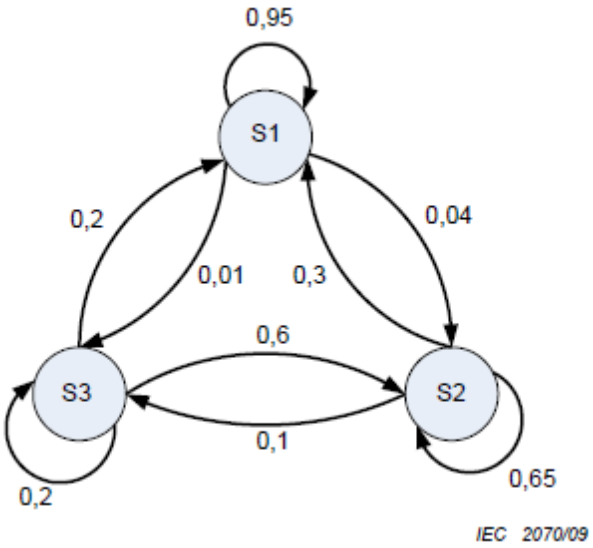
Tableau N°13: Matrice de Markov

		Etat aujourd'hui		
		S1	**S2**	**S3**
Etat demain	**S1**	0.95	0.3	0.2
	S2	0.04	0.65	0.6
	S3	0.01	0.05	0.2

Source: ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p166.

Ce tableau des probabilités est appelé matrice de Markov, ou matrice de transition. Noter que la somme de chaque colonne est 1, étant donné qu'il s'agit de la somme de tous les résultats possibles dans chaque cas. Le système peut également être représenté par un diagramme de Markov, dans lequel les cercles et les flèches représentent respectivement les états et la transition avec la probabilité qui l'accompagne[1].

Figure N°41 : Exemple de diagramme de Markov du système



Source: ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p166.

En règle générale, les flèches partant d'un état vers lui-même ne sont pas affichées, mais elles le sont dans ces exemples, par souci d'exhaustivité.

Soit P*i*, représentant la probabilité de trouver le système à l'état *i* pour *i* = 1, 2, 3, les équations simultanées à résoudre étant:

P1 = 0,95 P1 + 0,30 P2 + 0,20 P3 (B.1)

P2 = 0,04 P1 + 0,65 P2 + 0,60 P3 (B.2)

P3 = 0,01 P1 + 0,05 P2 + 0,20 P3 (B.3)

Ces trois équations ne sont pas indépendantes et ne résoudront pas les trois inconnues. Il convient d'utiliser l'équation suivante, et d'éliminer l'une des équations ci-dessous.

1 = P1 + P2 + P3 (B.4)

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p 166.

La solution est 0,85, 0,13 et 0,02 pour les états respectifs 1, 2, 3. Le système fonctionne complètement pendant 85 % du temps, à l'état dégradé pendant 13 % du temps et est en panne pendant 2 % du temps.

Pour les événements continus, soit deux éléments fonctionnant en parallèle devant être opérationnels pour que le système fonctionne. Les éléments peuvent être opérationnels ou en panne, et la disponibilité du système dépend de l'état des éléments.

Les états peuvent être les suivants:

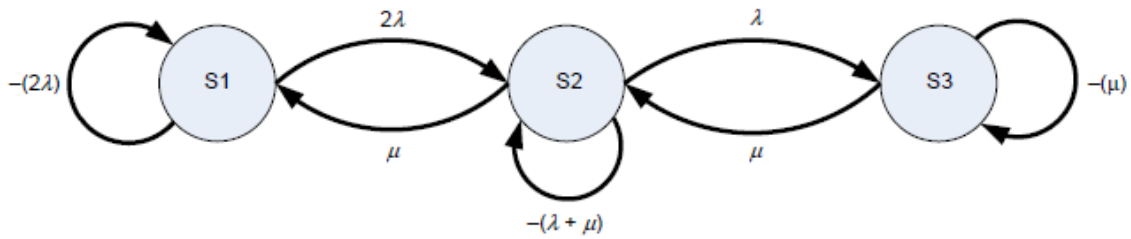
Etat 1 Les deux éléments fonctionnent correctement;

Etat 2 Un élément est tombé en panne et est en cours de réparation. L'autre élément fonctionne;

Etat 3 Les deux éléments sont tombés en panne et un 'élément est en cours de réparation.

Si le taux de défaillance continu de chaque élément est λ et que la fréquence de réparation est μ, le diagramme de transition d'état est donc:

Figure N°42 : Exemple de diagramme de transition d'état



Source : ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p167.

Noter que la transition de l'état 1 à l'état 2 est 2λ, étant donné que la défaillance de l'un ou l'autre des éléments fera passer le système à l'état 2.

Soit P*i*(*t*), la probabilité d'être à l'état *i* à l'instant *t*, et

Soit P*i*(*t* + *δt*), la probabilité d'être à l'état final à l'instant *t* + *δt*

La matrice de probabilité de transition devient:

Tableau N°14: Matrice de Markov finale

		Etat initial		
		P1(t)	**P2(t)**	**P3(t)**
	P1(t+δt)	-2λ	μ	0
Etat final	P2(t+δt)	2λ	-(λ+μ)	μ
	P3(t+δt)	0	Λ	-μ

Source: ISO/IEC 31010; Risk management-Risk Assessment Techniques ; p167.

Il convient de noter que les valeurs nulles sont probables, puisqu'il est impossible de passer de l'état 1 à l'état 3 ou inversement. De même, la somme des colonnes donne zéro lors de la spécification des taux.

Les équations simultanées deviennent:

$dP1/dt = -2\lambda\ P1(t) + \mu\ P2(t)$ (B.5)

$dP2/dt = 2\lambda\ P1(t) + -(\lambda + \mu)\ P2(t) + \mu\ P3(t)$ (B.6)

$dP3/dt = \lambda\ P2(t) + -\mu\ P3(t)$ (B.7)

Pour plus de simplicité, la disponibilité requise est supposée être celle à l'état stable.

Si δt tend vers l'infini, dPi/dt tend vers zéro, et les équations deviennent plus faciles à résoudre. Il convient également d'utiliser l'équation supplémentaire indiquée dans l'Équation (B.4) citée précédemment:

A présent, l'Équation $A(t) = P1(t) + P2(t)$ peut être exprimée sous la forme:

$A = P1 + P2$

De ce fait $A = (\mu 2 + 2\ \lambda\ \mu\ ) / (\ \mu 2 + 2\ \lambda\ \mu + \lambda 2)$

Le résultat d'une analyse de Markov est l'ensemble des différentes probabilités qu'un système se trouve dans différents états. Il s'agit donc d'une estimation des probabilités de défaillance et/ou disponibilité, l'un des composants essentiels d'un système.

L'analyse de Markov présente les avantages suivants:

- possibilité de calculer les probabilités pour des systèmes offrant des capacités de réparation et plusieurs états dégradés.

L'analyse de Markov présente les limites suivantes:

- hypothèse de probabilités constantes de modification de l'état: panne ou réparations;
- du point de vue statistique, tous les événements sont indépendants étant donné que les états à venir sont indépendants de tous les états passés, sauf pour l'état immédiatement antérieur;
- nécessite une bonne connaissance de toutes les probabilités de changement d'état;
- bonne connaissance des opérations matricielles;
- les résultats sont difficiles à communiquer au personnel non technique.

2.1.2. Benchmarking[1]

Lorsque le management cherche à améliorer les décisions prises en matière de traitement de risque, en vue de réduire la probabilité ou l'impact, des techniques de benchmarking peuvent être utilisées pour évaluer un risque spécifique en termes de probabilité d'occurrence et d'impact. Les données de référence utilisées dans le cadre du benchmarking offrent au management un aperçu de la probabilité et de l'impact des risques basés sur les antécédents d'autre organisation. Le benchmarking est également utilisés pour identifier des opportunités d'amélioration de processus.

Les activités de benchmarking comprennent :

- Interne: comparaison des mesures d'un département ou d'une division avec d'autre département et division appartenant à la même entité.
- Concurrence/secteur: comparaison avec les concurrents directs ou un groupe plus large d'organisation dont les caractéristiques sont similaires.
- Best-in-class : Examen des mesures parmi des organisations de différents secteurs.

[1] IFACI, PwC et Landwell; COSO-II Report : Op.cit; p 218.

2.1.3. Simulation de Monte-Carlo[1]

La plupart des systèmes sont trop complexes pour que l'on puisse modéliser les effets de l'incertitude, dont ils font l'objet, à l'aide de techniques analytiques. Cependant, ils peuvent être évalués en considérant les entrées comme des variables aléatoires et en procédant à un certain nombre N de calculs (appelés simulations) dans lesquels les entrées sont échantillonnées pour obtenir N résultats possibles du résultat souhaité.

Cette méthode peut résoudre des situations complexes qu'il serait difficile de comprendre et de résoudre par une méthode analytique. Les systèmes peuvent être développés à l'aide d'une feuille de calcul et d'autres outils conventionnels, mais des outils plus sophistiqués sont disponibles pour répondre aux exigences plus complexes, la plupart d'entre eux étant aujourd'hui peu onéreux. Lorsque la technique a été développée, le nombre d'itérations requises pour les simulations de Monte-Carlo ralentissait le processus et prenait beaucoup de temps; pourtant, les avancées informatiques et les développements théoriques (l'échantillonnage par hypercube latin, par exemple) ont considérablement réduit la durée de traitement pour la plupart des applications.

La simulation de Monte-Carlo offre un moyen d'évaluer les effets de l'incertitude sur les systèmes dans un large éventail de situations. D'une manière générale, elle est utilisée pour évaluer l'étendue des résultats possibles et la fréquence relative des valeurs dans cette étendue pour les mesures quantitatives d'un système (le coût, la durée, le débit, la demande et autres mesures analogues, par exemple). La simulation de Monte-Carlo peut être utilisée à deux fins différentes:

- projection de l'incertitude sur des modèles d'analyse conventionnels;
- calculs probabilistes lorsque des techniques d'analyse ne s'appliquent pas.

Une bonne compréhension du système et des informations sur les types d'entrée, les sources d'incertitude à représenter et le résultat requis sont nécessaires. Les données d'entrée liées à l'incertitude sont représentées comme des variables aléatoires dont les distributions sont plus ou moins réparties selon le niveau des incertitudes. Des distributions uniformes, triangulaires, normales et log-normales sont souvent utilisées à cette fin.

Le processus est le suivant:

a) Un modèle ou algorithme est défini pour représenter, le plus étroitement possible, le comportement du système étudié.

b) Le modèle est appliqué plusieurs fois en utilisant des nombres aléatoires pour générer des résultats du modèle (simulations du système). Lorsque l'application consiste à modéliser les effets de l'incertitude, le modèle se présente sous la forme d'une équation qui fournit la relation entre des paramètres d'entrée et un résultat en sortie. Les valeurs sélectionnées pour les entrées sont issues de distribution de probabilité appropriées qui représentent la nature de l'incertitude pour ces paramètres.

c) Dans tous les cas, un calculateur applique le modèle plusieurs fois (le plus souvent jusqu'à 10 000 fois) avec différentes entrées et génère plusieurs résultats en sortie. Ces résultats peuvent être traités au moyen de statistiques conventionnelles pour fournir des informations (valeurs moyennes, écarts types, intervalles de confiance, par exemple).

Il peut s'agir d'une seule valeur, telle que déterminée dans l'exemple ci-dessus, d'un résultat exprimé sous la forme d'une distribution des probabilités ou des fréquences, ou de

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; p168.

l'identification des principales fonctions du modèle dont l'impact sur le résultat est le plus important.

D'une manière générale, une simulation de Monte-Carlo est utilisée pour évaluer l'ensemble de la distribution des résultats ou les mesures-clés issues d'une distribution, comme[1] :

- la probabilité d'un résultat défini;
- la valeur d'un résultat dans laquelle les personnes concernées par le problème ont un certain niveau de confiance ne sera pas dépassé, un coût inférieur à 10 % de chance de dépasser ou une durée à 80 % certaine d'être dépassée.

Une analyse des relations qu'entretiennent les entrées et les résultats peut éclairer la signification relative des facteurs en cours et identifier les cibles utiles pouvant influencer l'incertitude du résultat.

L'analyse de Monte-Carlo présente les avantages suivants:

- en principe, la méthode peut concilier toutes les distributions dans une variable d'entrée, y compris les distributions empiriques déduites des observations de systèmes connexes;
- les modèles sont relativement simples à développer et peuvent être étendus à mesure de l'évolution des besoins;
- toutes les influences ou relations se produisant dans la réalité peuvent être représentées, y compris les effets subtils tels que les dépendances conditionnelles;
- l'analyse de sensibilité peut être appliquée pour distinguer les influences importantes de celles qui le sont moins;
- les modèles sont aisément compréhensibles étant donné que la relation entre les entrées et les résultats est transparente;
- des modèles de comportement efficaces tels que les réseaux de Pétri sont disponibles et se révèlent très efficaces pour la simulation de Monte-Carlo;
- elle fournit une mesure de l'exactitude d'un résultat;
- le logiciel est disponible et relativement peu onéreux.

Les limites sont les suivantes:

- l'exactitude des solutions dépend du nombre de simulations qu'il est possible de réaliser (cette limite est réduite grâce à l'amélioration des vitesses de calcul informatique);
- elle repose sur l'aptitude à représenter les incertitudes liées aux paramètres par une distribution valide;
- des modèles volumineux et complexes peuvent faire concurrence au programme de modélisation et rendre le début du processus difficile pour les différents acteurs;
- la technique peut ne pas distinguer correctement les conséquences élevées des événements peu probables et, par conséquent, ne pas permettre de refléter dans l'analyse la sensibilisation au risque d'une organisation.

2.2. Les méthodes qualitatives:

Certaines évaluations réalisées selon des techniques qualitatives sont exprimées en termes subjectifs alors que d'autre sont formulées en termes plus objectifs. Toutefois dans les deux

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; p168.

cas, la qualité de ces évaluations dépend essentiellement des connaissances et du discernement des personnes impliquées, de leur compréhension des événements potentiels et du contexte.

2.2.1. L'Analyse Préliminaire de Risque APR / Analyse Préliminaire de Danger ADP (Preliminary Hazard Analysis PHA)[1]

L'analyse Préliminaire de Risque (Danger) a été développée au début des années 1960 dans les domaines aéronautique et militaire.

Selon la norme CEI-300-3-9 (CEI 300-3-9, 1995) : « L'APR est une technique d'identification et d'analyse de la fréquence du danger qui peut être utilisée lors des phases amont de la conception pour identifier les dangers et évaluer leur criticité ».

Le but consiste à identifier les entités dangereuses d'un système, puis à regarder pour chacune d'elles comment elles pourraient générer un incident ou un accident plus ou moins grave suite à une séquence d'événements causant une situation dangereuse.

Pour identifier les entités et les situations dangereuses susceptibles d'en découler, l'analyste est aidé par des listes de contrôles (check-lists) d'entités dangereuses, de situations dangereuses et d'événements redoutés. Ces check-lists sont spécifiques au domaine d'étude concerné.

Comme son nom l'indique, cette méthode n'est pas destinée à traiter en détail la matérialisation des scénarios d'accident, mais plutôt à mettre rapidement en évidence les gros problèmes susceptibles d'être rencontrés pendant l'exploitation du système étudié.

Cependant, l'APR peut aussi et même doit être complétée par la plupart des analyses de risques fonctionnelles telles que l'AMDEC ou l'Arbre de Défaillances.

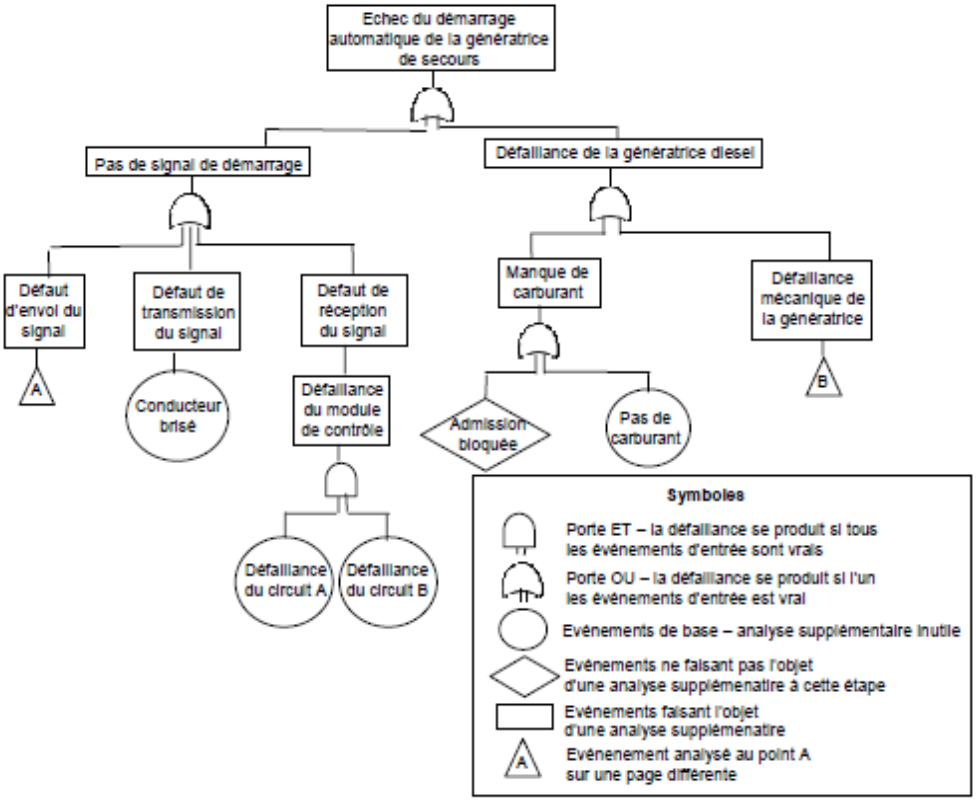
2.2.2. L'arbre des Défaillances [2]

L'arbre des défaillances est une méthode qui part d'un événement final (ENS) pour remonter vers les causes et conditions dont les combinaisons peuvent le provoquer. Il vise à représenter l'ensemble des combinaisons qui peuvent induire l'événement étudie d'ou sa représentation schématique. Les facteurs de causalité sont identifiés de manière déductive et organisés de manière logique et graphique, sous la forme d'une arborescence décrivant les facteurs de causalité et leurs relations logiques à l'événement de tête. On construit et on utilise un arbre de défaillance dans le cadre d'une étude a priori d'un système. Ayant pour point de départ un ENS (dysfonctionnement ou accident), la démarche consiste à s'appuyer sur la connaissance des éléments constitutifs du système étudie pour identifier tous les scenarios conduisant à cet ENS. Graphiquement (Figure n°43), un arbre de défaillance se représente en deux dimensions matérialisant les enchainements qui peuvent conduire à l'ENS. Cette représentation peut également être utilisée pour calculer la probabilité de l'événement redoute à partir des probabilités des événements élémentaires qui se combinent pour le provoquer.

[1] Mohamed –Habib Mazouni; Op.cit. p 50.

[2] Matthieu Desinde; Contribution à la mise au point d'une approche intégrée analyse diagnostique/analyse de risques; thèse de doctorat; université JOSEPH Fourier - GRENOBLE; Décembre 2006. P27.

Figure N°43: Représentation graphique d'un arbre de défaillance



Source : ISO/IEC 31010; Risk management-Risk Assessment Techniques ; p144.

Les combinaisons d'événements sont habituellement représentées par des portes logiques "ET", "OU", "ET" avec conditions, "OU" avec conditions, "SI" et des portes du type "ET m/n" (porte franchissable si m événements parmi n sont réalisés) [Limnios, 2005]. Par ailleurs, certains auteurs [Lievens, 1976] [Pages & Gondran, 1980] mentionnent d'autres portes logiques utilisées dans des applications particulières : porte "MATRICIELLE", porte "SOMMATION", etc...

Un arbre de panne peut être utilisé de manière qualitative pour identifier les causes et cheminements potentiels donnant lieu à une défaillance (l'événement de tête), ou de manière quantitative pour calculer la probabilité de l'événement de tête, compte tenu de la connaissance des probabilités des événements de causalité.

Il peut être utilisé à l'étape de la conception d'un système pour identifier les causes potentielles de défaillance et, par conséquent, faire un choix parmi les différentes options de conception. Il peut être utilisé à l'étape du fonctionnement pour identifier la manière dont les défaillances majeures peuvent se produire et l'importance relative des différents cheminements vers l'événement de tête. Un arbre de panne peut également être utilisé pour analyser une défaillance qui s'est produite afin d'afficher un graphique des différents événements à l'origine de la défaillance.

Pour l'analyse qualitative, une bonne compréhension du système et des causes de la défaillance est requise ainsi qu'une compréhension technique de la manière dont le système peut tomber en panne. Des diagrammes détaillés sont utiles pour faciliter l'analyse.

Pour l'analyse quantitative, les taux de défaillance ou la probabilité d'être en état de défaillance pour tous les événements de base de l'arbre de panne sont requis.

La procédure de développement de l'arbre de panne est la suivante[1]:

- L'événement de tête à analyser est défini. Il peut s'agir d'une défaillance ou du résultat plus général d'une défaillance. Si le résultat est analysé, l'arbre peut contenir une section portant sur la limitation de la défaillance réelle.

- En commençant par l'événement de tête, les causes possibles immédiates ou les modes de défaillance donnant lieu à l'événement de tête sont identifiés.

- Chacun de ces causes/modes de défaillance est analysé pour savoir comment la défaillance a pu se produire.

- En suivant progressivement l'identification du fonctionnement indésirable du système jusqu'aux niveaux système successivement inférieurs, l'analyse approfondie devient inutile. Dans un système matériel, il peut s'agir d'un niveau de défaillance du composant. Les événements et facteurs de causalité au niveau le plus bas du système analysé sont appelés événements de base.

- Si des probabilités peuvent être attribuées aux événements de base, il est possible de calculer la probabilité de l'événement de tête. Pour que la quantification soit valide, il doit être possible de démontrer que, pour chaque porte, toutes les entrées sont nécessaires et suffisantes pour produire l'événement de résultat. Si ce n'est pas le cas, l'arbre de panne n'est pas valide pour l'analyse de probabilité. Il peut néanmoins être un outil utile pour afficher les relations causales.

Dans le cadre de la quantification, il peut s'avérer nécessaire de simplifier l'arbre de panne à l'aide d'algèbre booléenne pour représenter les modes de défaillance en double.

Tout en fournissant une estimation de la probabilité de l'événement principal, des coupes minimales, faisant office de vecteurs individuels distincts vers l'événement principal, peuvent être identifiées et leur influence sur l'événement de tête calculée.

Sauf pour les arbres de panne simples, un progiciel est nécessaire pour réaliser correctement les calculs en présence d'événements répétés à plusieurs endroits dans l'arbre de panne, et pour calculer les coupes minimales. Les outils logiciels assurent la cohérence, l'exactitude et la vérifiabilité.

Les résultats de l'analyse par arbre de panne sont les suivants:

- une représentation graphique du déroulement de l'événement de tête, illustrant les vecteurs d'interaction par lesquels plusieurs événements simultanés peuvent se produire;

- une liste des coupes minimales (vecteurs individuels vers la défaillance) avec (lorsque les données sont disponibles) la probabilité de survenue de chacune d'elle;

- la probabilité de l'événement de tête.

Les avantages de l'analyse par arbre de panne sont les suivants:

- Elle constitue une approche disciplinée et hautement systématique, mais également suffisamment souple pour permettre d'analyser divers facteurs, y compris les interactions humaines et les phénomènes physiques.

- L'application de l'approche «du haut vers le bas», implicite dans la technique, met l'accent sur les effets de défaillance qui sont en rapport direct avec l'événement de tête.

- L'analyse par arbre de panne est particulièrement utile à l'analyse de systèmes disposant de nombreuses interfaces et interactions.

1 ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit; p144.

• La représentation graphique permet de comprendre plus facilement le comportement du système et de ses facteurs inhérents, bien que la taille souvent importante des arbres puisse nécessiter un traitement informatique. Cette fonction permet d'inclure des relations logiques plus complexes (par exemple ET OU NON EXCLUSIF), mais rend également la vérification de l'arbre de panne plus difficile.

• L'analyse logique des arbres de panne et l'identification des coupes sont utiles pour identifier les vecteurs de défaillance simples d'un système très complexe, dans lequel des combinaisons particulières d'événements donnant lieu à l'événement de tête peuvent être ignorées.

Les limites sont les suivantes:

• Les incertitudes liées aux probabilités des événements principaux sont prises en compte dans les calculs de la probabilité de l'événement de tête. Ceci peut donner lieu à des niveaux élevés d'incertitude lorsque les probabilités de défaillance de base ne sont pas connues avec exactitude. Cependant, il est possible d'obtenir un degré élevé de confiance pour un système bien compris.

• Dans certains cas, les événements de causalité ne sont pas liés, et il peut s'avérer difficile d'établir que tous les vecteurs importants menant vers l'événement de tête sont inclus. Par exemple, introduire comme événement de tête toutes les sources d'inflammation dans une analyse d'un incendie. Dans ce cas, l'analyse de probabilité est impossible.

• L'arbre de panne est un modèle statique; les interdépendances temporelles ne sont pas traitées.

• Les arbres de panne ne peuvent traiter que les états binaires (défaillant/non défaillant).

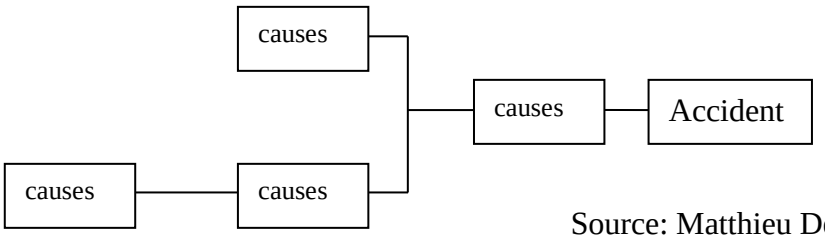
• L'erreur humaine pouvant être intégrée dans un arbre de panne qualitatif, il n'est généralement pas aisé d'inclure les défaillances dont le degré ou la qualité présentent souvent les signes d'une erreur humaine.

• Un arbre de panne ne permet pas d'intégrer aisément les effets domino ou les défaillances conditionnelles.

2.2.3. L'arbre des causes[1]

L'arbre des causes part d'un événement qui s'est produit et organise l'ensemble des événements ou conditions qui se sont combines pour le produire. Il repose sur un raisonnement dans le même sens que l'arbre des défaillances mais ne décrit qu'un seul scenario. Il se représente également en deux dimensions :

Figure N°44: Représentation graphique d'un arbre des causes

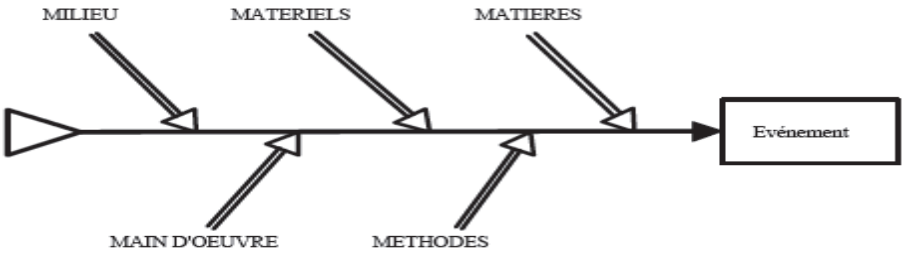


Source: Matthieu Desinde; op.cit. p28.

On construit un arbre des causes en générale dans une démarche de retour d'expérience. Lors de la recherche des causes, on peut s'appuyer sur l'arbre d'Ishikawa qui donne une méthode pour détailler tous les facteurs possibles liés à un événement indésirable

[1] Matthieu Desinde; Op.cit. p 28.

Figure N°45 : Arbre d'ishikawa



Source**:** Matthieu Desinde; op.cit. p28.

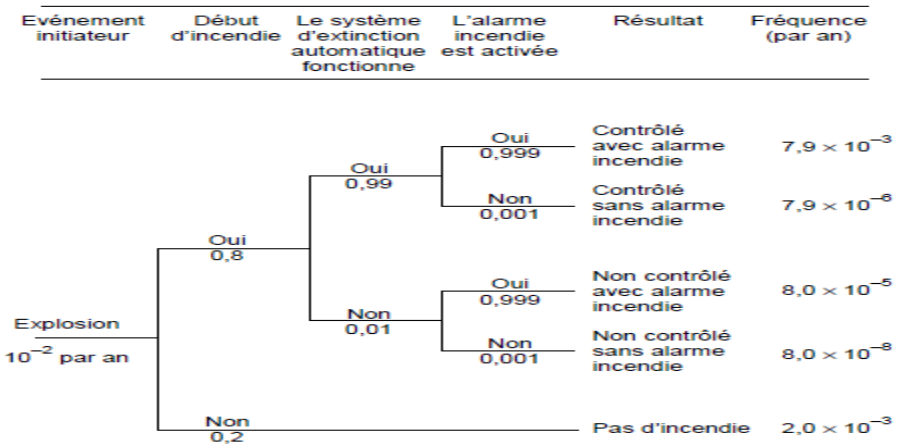
Quel arbre choisir[1]?

L'arbre des défaillances a pour objectif de mettre en exergue les points vulnérables d'une installation dont les défaillances pourraient être à l'origine d'un événement indésirable. Dans ce type d'analyse, on cotera chaque événement de l'arbre par des probabilités de manière à rechercher les coupes minimales. D'un autre cote, l'arbre des causes cherche à analyser une situation (un accident par exemple) à posteriori à partir d'événements passes provenant d'analyses "post-accident". L'arbre des causes cherche à expliquer l'événement indésirable qui s'est produit alors que l'arbre des défaillances cherche à déterminer les points faibles pour éviter un événement indésirable particulier.

2.2.4. L'arbre des événements

L'analyse par arbre d'événements est une technique graphique permettant de représenter les séquences d'événements mutuellement exclusifs suivant un événement initiateur en fonction du fonctionnement/non fonctionnement des divers systèmes conçus pour limiter ses conséquences. Elle peut être appliquée de manière qualitative et quantitative.

Figure N°46: Exemple d'arbre d'événement



Source: ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p147.

La Figure 46 illustre des calculs simples d'un exemple d'arbre d'événements lorsque les nœuds sont totalement indépendants.

En se déployant comme un arbre, l'AAE permet de représenter les événements aggravants ou limiteurs résultant de l'événement initiateur, en tenant compte des systèmes, fonctions ou barrières supplémentaires.

[1] Matthieu Desinde; op.cit ; p28.

L'AAE peut être utilisée pour modéliser, calculer et classer (du point de vue des risques) différents scénarii d'accidents à la suite d'un événement initiateur.

L'analyse par arbre d'événements peut être utilisée à toutes les étapes du cycle de vie d'un produit ou d'un processus. Elle peut être utilisée de manière qualitative pour faciliter la conception de scénarii potentiels et de séquences d'événements à la suite d'un événement initiateur, et déterminer dans quelle mesure les résultats sont affectés par différents traitements, barrières et contrôles destinés à limiter les résultats indésirables.

L'analyse quantitative se prête à la prise en compte de l'admissibilité des contrôles. Elle permet le plus souvent de modéliser les défaillances, lorsque plusieurs dispositifs de protection sont en place.

L'AAE peut être utilisée pour modéliser les événements initiateurs à l'origine de pertes ou de gains. Toutefois, les circonstances de recherche des vecteurs d'optimisation des gains sont plus souvent modélisées dans un arbre de décision.

Les entrées sont les suivantes[1]:

- une liste des événements initiateurs appropriés;
- des informations sur les traitements, les barrières et les contrôles, et leurs probabilités de défaillance (pour des analyses quantitatives);
- une compréhension des processus par lesquels une défaillance initiale s'aggrave.

Un arbre d'événements débute par la sélection d'un événement initiateur. Il peut s'agir d'un incident (une explosion due à la poussière, par exemple) ou d'un événement de causalité (une coupure d'alimentation, par exemple). Les fonctions ou systèmes en place pour limiter les résultats sont alors indiqués en séquence. Pour chaque fonction ou système, une droite est tracée pour représenter leur succès ou leur défaillance. Une probabilité particulière de défaillance peut être attribuée à chaque droite, cette probabilité conditionnelle étant estimée par l'avis d'un expert ou une analyse par arbre de panne, par exemple. De cette manière, différents vecteurs partant de l'événement initiateur sont modélisés.

Il est à noter que les probabilités de l'arbre d'événements sont conditionnelles, ce qui signifie par exemple que la probabilité de fonctionnement d'une installation fixe d'extinction automatique n'est pas la probabilité obtenue à partir des essais réalisés dans des conditions normales, mais la probabilité de fonctionnement dans des conditions d'incendie dû à l'explosion.

Chaque chemin traversant l'arbre représente la probabilité de survenue de tous les événements dudit chemin. Par conséquent, la fréquence du résultat est représentée par le produit des probabilités conditionnelles individuelles et de la fréquence de l'événement initiateur, étant donné que les différents événements sont indépendants.

Les résultats de l'analyse par arbre d'événements sont les suivants [2]:

- descriptions qualitatives des problèmes potentiels par combinaison des événements générant différents types de problèmes (étendue des résultats) issus d'événements initiateurs;
- estimations quantitatives des fréquences ou probabilités d'événement et importance relative des différentes séquences de défaillance et événement contributifs;
- listes des recommandations permettant de réduire les risques;
- évaluations quantitatives de l'efficacité des recommandations.

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p147.
[2] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p147.

Les avantages de l'analyse par arbre d'événements sont les suivants[1] :

- AAE permet un affichage graphique clair des scénarii potentiels analysés à la suite d'un événement initiateur et de l'impact du succès ou de l'échec des systèmes ou fonctions palliatifs;
- elle représente la durée, la dépendance et les effets domino qui gênent la modélisation des arbres de panne;
- elle représente de manière graphique les séquences d'événements qu'il n'est pas possible de représenter avec les arbres de panne.

Les limites sont les suivantes [2]:

- pour utiliser l'analyse par arbre d'événements dans le cadre d'une évaluation cohérente, il est indispensable d'identifier tous les événements initiateurs potentiels. Ceci peut être réalisé en utilisant une autre méthode d'analyse (HAZOP, APD, par exemple), cependant, cette technique comporte toujours un risque d'omission de certains événements initiateurs importants.
- les arbres d'événements traitent uniquement des états de succès et de défaillance d'un système, et il est difficile d'y intégrer des événements de succès ou de récupération différés;
- tous les vecteurs sont conditionnels pour les événements se produisant sur des nœuds précédents le long du vecteur. La plupart des dépendances le long des vecteurs possibles sont donc résolues. Toutefois, certaines dépendances (les composants communs, les systèmes utilitaires et les opérateurs, par exemple) peuvent être ignorées, donnant lieu à des estimations optimistes du risque si elles ne sont pas correctement traitées.

2.2.5. Analyse des Modes de Défaillances, de leurs Effets AMDE/ et de leur Criticité AMDEC [3]:

L'AMDE est une technique permettant d'identifier dans quelles mesures les composants, les systèmes ou les processus peuvent tomber en panne pour exécuter la conception prévue. Elle a été employée pour la première fois dans le domaine de l'industrie aéronautique durant les années 1960, son utilisation s'est depuis répandue à d'autres secteurs industriels. L'AMDEC est l'extension naturelle de l'étude AMDE quand il est question d'évaluer la criticité des défaillances, elle considère la probabilité d'occurrence de tous les modes de défaillance et la gravité des effets pour hiérarchiser les criticités.

L'AMDE permet d'identifier:

- tous les modes de défaillance potentiels des différentes parties d'un système (un mode de défaillance est l'observation d'une panne ou de ce qui ne fonctionne pas correctement);
- les effets que ces défaillances peuvent avoir sur le système;
- les causes de la défaillance;
- la manière d'éviter les défaillances et/ou de limiter leurs effets sur le système.

La méthode AMDEC développe une AMDE de sorte que chaque mode de défaillance identifié soit classé conformément à son importance ou criticité.

D'une manière générale, il s'agit d'une analyse qualitative ou semi-quantitative, mais qui peut être quantifiée à l'aide des taux de défaillance actuels.

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p147.
[2] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p147.
3 Idem; p140.

Il existe plusieurs types de méthode AMDE: l'AMDE Conception (ou produit), qui est utilisée pour les composants et les produits, l'AMDE Système utilisée pour les systèmes, l'AMDE Processus utilisée pour les processus de fabrication et d'assemblage, l'AMDE Service et l'AMDE Logiciel.

L'AMDE/AMDEC peut être appliquée lors de la conception, de la fabrication ou du fonctionnement d'un système.

Toutefois, pour améliorer la sûreté de fonctionnement, il est généralement plus aisé de mettre en œuvre les modifications lors de la phase de conception. L'AMDE et l'AMDEC peuvent également être appliquées aux processus et aux procédures. Elle est par exemple utilisée pour identifier le potentiel d'erreur médicale dans les systèmes de soins de santé et de défaillances dans les procédures de maintenance.

L'AMDE/AMDEC peut être utilisée pour [1] :

- faciliter la sélection d'alternatives de conception à haute sûreté de fonctionnement,
- S'assurer que tous les modes de défaillance des systèmes et processus, et leurs effets sur le succès opérationnel ont été pris en compte,
- identifier les modes de défaillance humaine et leurs effets,
- fournir un socle de planification des essais et de la maintenance des systèmes physiques,
- améliorer la conception des procédures et des processus,
- fournir des informations qualitatives ou quantitatives pour les techniques d'analyse, telles que l'analyse par arbre de panne.

L'AMDE/AMDEC peut apporter des éléments d'entrée à d'autres techniques d'analyse

(L'analyse par arbre de panne, par exemple) du point de vue qualitatif ou quantitatif.

L'AMDE et l'AMDEC requièrent des informations suffisamment détaillées relatives aux composants du système pour permettre de procéder à une analyse significative des manières dont chaque composant peut tomber en panne. Pour une AMDE Conception détaillée, l'élément peut se situer au niveau détaillé de composant individuel alors que pour une AMDE Système de niveau supérieur, les éléments peuvent être définis à un niveau plus élevé.

Ces informations peuvent comprendre [2] :

- des schémas ou un organigramme du système en cours d'analyse et de ses composants, ou les étapes d'un processus;
- une bonne compréhension de la fonction de chaque étape d'un processus ou d'un composant d'un système;
- les détails du processus et des paramètres environnementaux, susceptibles d'affecter le fonctionnement;
- une compréhension des résultats liés à des défaillances particulières;
- des informations historiques relatives aux défaillances, comprenant les taux de panne calculés, le cas échéant.

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p140.
[2] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p140.

Les étapes de l'analyse AMDE sont les suivantes [1]:

a) définition du domaine d'application et des objectifs de l'étude;

b) constitution de l'équipe;

c) compréhension du système/processus faisant l'objet de l'analyse AMDEC;

d) décomposition du système en ses composants ou en étapes;

e) définition de la fonction de chaque étape ou composant;

f) pour chaque composant ou étape, répondre aux questions suivantes:

- est-il concevable qu'un composant tombe en panne?
- quels sont les mécanismes susceptibles de produire ces modes de défaillance?
- quels seraient les effets d'éventuelles défaillances?
- la défaillance est-elle anodine ou dangereuse?
- comment la défaillance a-t-elle été détectée?

g) Identifier des dispositions inhérentes dans la conception pour compenser la défaillance.

Pour l'analyse AMDEC, l'équipe chargée de l'étude classe chacun des modes de défaillance identifiés en fonction de sa criticité.

Ceci peut être réalisé de plusieurs manières. Les méthodes courantes sont les suivantes:

- l'indice de criticité du mode;
- le niveau de risque;
- le degré de priorité du risque.

Le modèle de criticité est une mesure de la probabilité que le mode considéré donnera lieu à une défaillance du système dans son ensemble; il est défini comme suit:

Probabilité d'effet de défaillance * Taux de défaillance de mode * Temps de fonctionnement du système

Il est le plus souvent appliqué aux défaillances d'équipement pour lesquelles chacun de ces termes peut être défini de manière quantitative et les modes de défaillance ont tous la même conséquence.

Le niveau de risque est obtenu en combinant les conséquences d'un mode de défaillance et la probabilité de défaillance. Il est utilisé lorsque les conséquences des différents modes de défaillance ne sont pas les mêmes et il peut être appliqué aux systèmes ou processus des équipements. Le niveau de risque peut être exprimé de manière qualitative, semi-quantitative ou quantitative.

Le degré de priorité du risque (NRP) est une mesure semi-quantitative de la criticité obtenue en multipliant les nombres des échelles de classement (généralement comprise entre 1 et 10) correspondant à la conséquence de la défaillance, probabilité de défaillance et aptitude à détecter le problème. (Une priorité élevée est attribuée à une défaillance en cas de difficulté de détection.) Cette méthode est le plus souvent utilisée dans des applications d'assurance de qualité.

Une fois identifiés les modes et mécanismes de défaillance, il est possible de définir et de mettre en œuvre des actions correctives pour les modes de défaillance les plus significatifs.

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p140.

L'AMDE est documentée dans un rapport contenant :

- les caractéristiques du système analysé;
- la manière dont l'analyse a été réalisée;
- les hypothèses avancées dans l'analyse;
- les sources des données;
- les résultats, y compris les fiches de travail renseignées;
- la criticité (si traitée) et la méthodologie utilisée pour la définir;
- toutes les recommandations pour des analyses approfondies, des changements de conception ou des fonctions à intégrer dans les plans d'essai, etc.

Le système peut être réévalué par un autre cycle d'analyse AMDE, à l'issue des actions entreprises.

Le principal résultat de l'analyse AMDE est une liste des modes de défaillance, des mécanismes de défaillance et des effets pour chaque composant d'un système ou étape d'un processus (qui peut inclure des informations sur la probabilité de défaillance). Des informations sont également données sur les causes de la défaillance et ses conséquences sur l'ensemble du système. Les résultats de l'analyse AMDEC incluent une évaluation de l'importance fondée sur la probabilité de défaillance du système, le niveau de risque résultant du mode de défaillance ou une combinaison du niveau de risque et de « l'aptitude à la détection » du mode de défaillance.

L'analyse AMDEC peut donner un résultat quantitatif lorsqu'on utilise des données de taux de défaillance appropriées et des conséquences quantitatives.

Les analyses AMDE/AMDEC présentent les avantages suivants [1]:

- Elles s'appliquent largement aux modes de défaillance humaine, d'équipements et de systèmes ainsi qu'aux matériels, logiciels et procédures;
- elles permettent d'identifier les modes de défaillance du composant, leurs causes et leurs effets sur le système, et de les présenter dans un format lisible;
- elles permettent d'éviter les modifications onéreuses de l'équipement en service par une identification précoce des problèmes dans le processus de conception;
- elles permettent d'identifier les modes de défaillance localisée et les exigences pour les systèmes redondants et de sécurité;
- elles offrent une entrée aux programmes d'essai de développement en mettant en évidence les fonctions essentielles à tester.

Les limites sont les suivantes:

- elles peuvent uniquement être utilisées pour identifier les modes de défaillance localisée, et pas les combinaisons de modes de défaillance;
- si les études ne sont pas convenablement contrôlées et mises au point, elles peuvent prendre du temps et être onéreuses;
- elles peuvent s'avérer difficiles et fastidieuses pour les systèmes complexes à plusieurs couches.

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p140.

2.2.6. Hazard and Operability Study (HAZOP)[1]

HAZOP est l'acronyme de Hazard and Operability Study (Etude de danger et d'exploitation). Il s'agit de l'examen structuré et systématique d'un produit. L'HAZOP a été initialement développée par la société "Imperial Chemical Industries" au début des années 1970 et s'applique à l'industrie. Elle sert à évaluer les dangers potentiels résultants des dysfonctionnements d'origine humaine ou matérielle et aussi les effets engendrés sur le système. Cette méthode a pour objectifs d'identifier les risques auxquels sont confrontés les personnes, les équipements, l'environnement et/ou les objectifs de l'organisation, et qui mènent à des événements dangereux lors d'une déviation des conditions normales de fonctionnement.

Le processus HAZOP est une technique qualitative reposant sur l'utilisation de mots-guides permettant de déterminer dans quelle mesure il n'est pas possible d'obtenir la conception ou les conditions de fonctionnement désirées à chaque étape de la conception, du processus, du mode opératoire ou du système. D'une manière générale, elle est mise en place par une équipe pluridisciplinaire à la suite de plusieurs réunions.

L'analyse HAZOP ressemble à l'analyse AMDE puisqu'elle identifie les modes de défaillance d'un processus, d'un système ou d'un mode opératoire, ainsi que leurs causes et leurs conséquences. La différence est que l'équipe tient compte des résultats et écarts indésirables par rapport aux résultats et conditions prévus, et revient aux causes et modes de défaillance possibles, tandis que l'analyse AMDE commence par identifier les modes de défaillance.

Lorsqu'une déviation est identifiée, l'analyse tente d'identifier les conséquences qui en découlent. Les déviations potentiellement dangereuses sont ensuite hiérarchisées en leur associant des actions de contrôle allouées. La méthode se termine par l'investigation des causes potentielles des déviations jugées crédibles.

De manière générale, les paramètres sur lesquels porte l'analyse sont observables, quantifiables et comparables. Par exemple la vitesse, la température, la pression, le débit, le niveau, le temps, etc.

La combinaison de ces paramètres avec des mots clés prédéfinis (plus que, moins que, pas de, etc.) se fait de la manière suivante :

« Plus de » et « Pression » = « Pression trop haute » / « Pas de » et « Niveau » = « Capacité vide ».

Dans le cas où une estimation de la criticité est nécessaire, HAZOP peut être complétée par une analyse quantitative simplifiée.

Une analyse HAZOP présente les avantages suivants[2]:

- offre le moyen d'examiner de manière systématique et rigoureuse un système, un processus ou un mode opératoire;
- implique la constitution d'une équipe pluridisciplinaire, composée de personnes aux compétences opérationnelles pragmatiques et en mesure de procéder à des opérations de traitement;
- génère des solutions et des moyens de traitement du risque;
- est applicable à un large éventail de systèmes, de processus et de modes opératoires;
- permet d'aborder de manière explicite les causes et conséquences d'une erreur humaine;

[1] Mohamed –Habib Mazouni; Op.cit. p 51.

2 ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p127.

- permet d'enregistrer par écrit le processus qui peut être utilisé pour éviter les actes de négligence.

Les limites sont les suivantes:

- elle peut prendre beaucoup de temps et donc être onéreuse;
- elle nécessite un niveau élevé de documentation ou de spécification de système/processus et de mode opératoire;
- l'attention peut porter exclusivement sur la recherche de solutions plutôt que sur les raisons qui motivent une action (ceci peut être limité par une approche progressive);
- la discussion peut porter essentiellement sur des détails de conception et non sur des questions plus larges ou externes;
- elle est limitée par le projet de conception et la conception elle-même, ainsi que par le domaine d'application et les objectifs imposés à l'équipe;
- le processus s'appuie fortement sur l'expertise des concepteurs, ces derniers pouvant trouver difficile de rester suffisamment objectifs quant aux problèmes que peuvent présenter leurs conceptions.

2.2.7. La méthode MOSAR[1]

La méthode MOSAR (Méthode Organisée et Systémique d'Analyse des Risques) a été mise au point par Pierre PERILHON au CEA. Elle est utilisée dans divers domaines, en particulier dans l'étude des risques d'installations à hauts risques (nucléaire, chimique, etc.). En effet, la méthode à été effectivement appliquée dans le domaine nucléaire et notamment à EDF (Centres de recherches et d'essais) et au CEA (Installations d'essais).

MOSAR contient deux modules hiérarchiques, un module macro « module 'A' » et un module micro « module 'B' ».

Le module 'A' a pour but d'identifier les dysfonctionnements techniques et opératoires provoquant un événement indésirable. Les scénarios d'accident sont examinés d'une manière macroscopique, autrement dit, sans traiter en détail des aspects fonctionnels du système et de ses interfaces. Principalement, le module 'A' se décompose en 6 étapes :

- Modélisation de l'installation.
- Identification des sources de danger.
- Identification des scénarios d'accident.
- Evaluation des scénarios de risque.
- Négociation des objectifs.
- Définition des moyens de maîtrise des risques.

Le module 'A' s'appuie essentiellement sur le modèle MADS dans la phase d'identification des sources, flux et cibles de dangers ainsi que les différents événements du processus de danger.

Le module B de la méthode MOSAR qui se présente d'ailleurs comme une suite logique du module A. Il permet d'effectuer une analyse plus détaillée des dysfonctionnements techniques et opératoires et aussi de l'impact qu'ils pourraient engendrer sur le système global. Ce module se décompose en 5 étapes :

[1] Mohamed –Habib Mazouni; Op.cit. p 56

- Identification des risques de dysfonctionnement.
- Evaluation des risques en constituant des Arbres de Défaillances.
- Négociation des objectifs précis de maîtrise des risques.
- Affinement des moyens complémentaires de maîtrise des risques.
- Management des risques.

2.3. Autre méthodes pour le management du risque au sein de l'entreprise

Comme on a vu dans l'élément précédent, nous avons présenté les méthodes relatives aux approches d'analyse des risques, cependant il y en a d'autres méthodes d'analyses de risque nous les présenterons comme suit:

2.3.1. « Brainstorming»[1]:

Le «brainstorming» implique de stimuler et d'encourager la libre conversation au sein d'un groupe de personnes compétentes afin d'identifier les modes de défaillance potentiels et les dangers, risques, critères de décision et/ou options de traitement associés. Le terme «brainstorming» est souvent utilisé très librement pour signifier tout type de discussion en groupe. Toutefois, le véritable «brainstorming» implique des techniques particulières dont l'objet est de stimuler l'imagination des personnes à l'aide des idées et déclarations des autres membres du groupe.

Une facilitation efficace est très importante dans cette technique. Elle comprend: la stimulation de la discussion au démarrage, l'encouragement périodique du groupe à évoquer d'autres domaines pertinents et la saisie des questions émanant de la discussion (qui est en général assez vivante).

Le «brainstorming» peut être utilisé avec d'autres méthodes d'évaluation des risques décrites ci-dessous. Il peut également être utilisé seul, comme une technique stimulant l'imagination à toutes les étapes du processus de management des risques et du cycle de vie d'un système. Il peut être utilisé dans le cadre de discussions de haut niveau dans lesquelles les problèmes sont identifiés, d'un examen plus détaillé ou d'un niveau approfondi lié à des problèmes particuliers.

Le «brainstorming» accorde une place prépondérante à l'imagination. Par conséquent, il est particulièrement utile lors de l'identification des risques liés à de nouvelles technologies, en l'absence de données ou lorsqu'il est nécessaire de trouver des solutions originales à des problèmes.

Le «brainstorming» peut être formel ou informel. Le «brainstorming» formel est plus structuré avec des participants préparés à l'avance, l'objectif et le résultat de la session étant définis, et des moyens étant prévus pour évaluer les idées avancées. Le «brainstorming» informel est moins structuré et souvent plus approprié.

Dans un processus formel :

- avant la session, le facilitateur prépare les éléments de réflexion correspondant au contexte;
- les objectifs de la session sont définis et les règles expliquées;
- le facilitateur avance une série d'éléments de réflexion. Chacun explore des idées en identifiant autant de problèmes que possible. A cette étape, aucune discussion n'est engagée, car il ne s'agit pas de savoir s'il convient que tel ou tel élément fasse partie d'une liste ou ce

1 ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p119.

que signifie une déclaration particulière, ce type de situation ayant tendance à bloquer la fluidité de la réflexion. Toutes les entrées sont acceptées, aucune ne faisant l'objet de critiques. Le groupe avance rapidement pour développer des pensées latérales;

- le facilitateur peut engager les personnes sur de nouvelles pistes lorsque la réflexion a été poussée suffisamment loin ou qu'elle s'écarte trop du sujet. Toutefois, il s'agit de rassembler autant d'idées diverses que possible en vue d'une analyse ultérieure.

Les résultats dépendent de l'étape du processus de management des risques dont il s'agit. Par exemple, à l'étape de l'identification, les résultats peuvent être une liste de risques et de contrôles actuels.

Les avantages du «brainstorming» sont les suivants:

- il stimule l'imagination et permet donc d'identifier de nouveaux risques et des solutions originales;
- il implique des acteurs clés et facilite donc la communication globale;
- il est relativement rapide et facile à mettre en place.

Les limites sont les suivantes:

- les participants peuvent manquer de compétences ou de connaissances pour être des contributeurs efficaces;
- étant donné qu'il est relativement peu structuré, il est difficile de démontrer que le processus est exhaustif (que tous les risques potentiels ont été identifiés, par exemple);
- il peut exister une dynamique de groupe variable, les personnes ayant des idées valables ne s'exprimant pas ou d'autres dominant la discussion. Cette situation peut être résolue par le «brainstorming» informatique, par l'intermédiaire d'un forum de discussion ou d'une technique de groupe nominal. Le «brainstorming» informatique peut être mis en place de manière anonyme, ce qui permet d'éviter les questions personnelles et politiques susceptibles de gêner le libre débat d'idées. Pour la technique de groupe nominal, les idées sont soumises de manière anonyme à un animateur et elles sont ensuite traitées par le groupe.

2.3.2. Analyse de Fiabilité Humaine (AFH)[1]

L'analyse de fiabilité humaine (AFH) porte sur l'impact des personnes sur les performances du système. Elle peut être utilisée pour évaluer les influences de l'erreur humaine sur le système.

La plupart des processus se caractérisent par des potentiels d'erreur humaine, plus particulièrement lorsque le temps dont dispose l'opérateur pour prendre une décision est court. La probabilité d'évolution d'un problème vers un événement plus sérieux peut être réduite. Toutefois, l'action humaine est parfois le seul rempart contre l'évolution d'une défaillance initiale vers un accident.

L'importance de la méthode AFH a été illustrée par différents accidents au cours desquels des erreurs humaines critiques ont contribué au déclenchement d'une séquence d'événements catastrophique. Ces accidents sont des alertes, mettant en garde contre les évaluations des risques portant uniquement sur les éléments matériels et logiciels d'un système. Ils illustrent les dangers de l'ignorance des possibilités d'erreur humaine. De plus, la méthode AFH est utile pour mettre en évidence les erreurs pouvant entraver la productivité, et pour révéler les moyens dont disposent les opérateurs et le personnel de maintenance pour «réparer» ces erreurs et autres défaillances (matérielles et logicielles).

1 ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p157.

La méthode AFH peut être utilisée de manière qualitative ou quantitative. Du point de vue qualitatif, elle permet d'identifier le potentiel d'erreur humaine et ses causes, de façon à réduire la probabilité d'erreur. Du point de vue quantitatif, elle permet de fournir des données sur les défaillances humaines dans l'analyse par arbre de panne ou d'autres techniques.

Les entrées de la méthode AFH sont les suivantes:

- informations permettant de définir les tâches qu'il convient que les personnes réalisent;
- expérience des types d'erreur se produisant dans la pratique et du potentiel d'erreur;
- compétence en matière d'erreur humaine et sa quantification.

Le processus AFH est le suivant[1] :

- **Définition du problème**, quels types d'implication humaine doivent être recherchés/évalués ?
- **Analyse des tâches,** comment sera réalisée la tâche et quel type d'aide sera nécessaire pour être performant ?
- **Analyse de l'erreur humaine,** comment la tâche peut-elle échouer: quelles erreurs peuvent être commises et comment peuvent-elle être réparées ?
- **Représentation**, comment intégrer ces erreurs ou défaillances de performances de tâche à d'autres événements matériels, logiciels ou environnementaux afin de calculer les probabilités de défaillance de l'ensemble du système ?
- **Dépistage**, existe-t-il des erreurs ou des tâches ne nécessitant pas de quantification détaillée ?
- **Quantification**, quelle est la probabilité d'erreurs individuelles et de défaillances des tâches ?
- **Evaluation de l'impact**, quelles sont les erreurs ou les tâches les plus importantes (en d'autres termes, quelles sont celles contribuant de manière la plus importante à la fiabilité ou au risque) ?
- **Réduction de l'erreur**, comment obtenir une meilleure fiabilité humaine ?
- **Documentation**, quelles caractéristiques de la méthode AFH doivent être documentées ?

Dans la pratique, le processus AFH se déroule par étape bien que, parfois, des étapes (L'analyse des tâches et l'identification des erreurs, par exemple) s'effectuent en parallèle.

Les résultats comprennent:

- une liste d'erreurs susceptibles de se produire et des méthodes permettant de les résoudre (par reprise de la conception du système, de préférence);
- modes d'erreur, causes et conséquences des types d'erreur;
- évaluation qualitative ou quantitative du risque posé par les erreurs.

Les avantages de l'analyse de fiabilité humaine sont les suivants:

1 ISO/IEC 31010; Risk management-Risk Assessment Techniques; Op.cit ; p157.

- elle propose un mécanisme formel permettant d'inclure l'erreur humaine dans la prise en compte des risques liés aux systèmes dans lesquels l'intervention humaine joue un rôle prépondérant;
- la prise en compte formelle des modes d'erreurs humaines et de leurs mécanismes peut permettre de réduire la probabilité de défaillance due à l'erreur.

Les limites sont les suivantes:

- la complexité et la variabilité humaines rendent difficile la définition de modes et probabilités de défaillance simples;
- la plupart des activités humaines ne disposent pas de mode réussite/échec simple. L'analyse de fiabilité humaine traite difficilement des défaillances partielles ou des défaillances liées à la qualité ou aux mauvaises décisions.

2.3.3. L'amélioration des processus[1]

Un processus correspond à toute série d'activités produisant des biens et services ou de l'information. L'idée de contrôler la variabilité d'un processus remonte à Walter A. Shewhart, inventeur du diagramme de contrôle en 1924. Pour améliorer des processus, on utilise notamment des diagrammes destinés à contrôler la qualité des produits, qualité à laquelle correspond une note, de sorte à s'assurer que les pièces sont conformes à un certain standard.

C'est le cas par exemple de la compagne de John Deere qui utilise un diagramme appelé « x barre» qui permet de s'assurer que toutes les pièces produites par l'entreprise sont conformes, en termes de qualité et que celles-ci correspondent aux promesses faites aux clients. Cette vérification se fait en examinant un produit fini en fonction d'une liste définissant les principales qualités du produit.

On attribue une note au produit à partir d'un barème de satisfaction, note portée sur le diagramme de contrôle. Si la note attribuée est comprise entre certaines limites, la production continue; au cas contraire, le processus de production est stoppé, le produit défectueux est examiné et le problème est rectifié.

2.3.4. La qualité totale[2]

Appelée aussi «zéro défaut », cet outil est une évolution de l'utilisation des diagrammes. En effet, inventé et développé par Joseph M. Juran et W. Edwards Deming, le concept de *«qualité totale»* est le stade ultime de la réduction de variabilité jusqu'à atteindre le zéro défaut et ce, bien au-delà du simple processus de production. Ce sont les fabricants japonais qui ont adopté et perfectionné cette technique ultime d'amélioration des processus induisant une réduction du risque; l'idée était de ne pas à avoir à investir dans le contrôle des processus dans la mesure où ceux-ci sont rendus efficaces et sûrs dès la phase de design et conception du produit.

Par ailleurs, il n'est nullement question d'investir massivement pour atteindre la qualité totale mais bien d'améliorer perpétuellement, de manière incrémentielle chaque activité de l'entreprise ce qui conduit à la diminution des divers risques. Un des exemples les plus célèbres d'utilisation de cet outil est la méthode « Six Sygma » inventée et utilisée par Motorola dans le but de maîtriser la variabilité des processus, bien au-delà de la production

[1] Olivier JENN; Outils de gestion du "Risque fournisseur" Méthodes et Modèles pour la sélection des fournisseurs; Décembre 2008; p76.
[2] Olivier JENN; Op.cit. p77.

dans le but de rendre la probabilité d'un défaut pratiquement égale à zéro. (Thomas Pyzdek, 1996). Le principe de qualité totale permet, en outre l'amélioration de la qualité des pièces et des matériaux achetés aux fournisseurs et ce, sans qu'aucun contrôle de l'entreprise ne soit nécessaire.

2.3.5. Le regroupement par lots[1]

Cet outil est d'avantage destiné aux opérations au-delà de la fabrication, notamment lors de l'expédition. A l'origine de cette méthode scientifique se trouve Jay forrester, un professeur au Massachusetts Institute of Technology et fondateur de la théorie de la dynamique des systèmes, qui a remarqué que la passation de commande entre les différents acteurs de la chaîne d'approvisionnement laissait entrevoir le risque d'augmentation de la variabilité de la commande initiale.

Le regroupement par lots consiste donc à réduire l'incertitude liée aux longs laps de temps existant entre deux commandes dans le cas d'un groupage des approvisionnements. L'objectif est donc de distiller les produits en lots plus petits mais de manière plus fréquente de sorte à fluidifier la chaîne d'approvisionnement. C'est ce type d'approvisionnement qui est notamment requis par les systèmes de livraison «juste-à-temps », courants dans l'industrie automobile.

La méthode de flexibilité [2]

Il existe constamment une part de «variabilité irréductible» qui est générée par les clients. L'objectif de cette méthode est de conserver en permanence la flexibilité dont l'entreprise a besoin pour faire face à cette variabilité. C'est le cas normalement pour Hewlett Packard avec le principe de retardement, qui consiste à «retarder» au maximum le moment où ses imprimantes produit seront différenciées pour répondre aux besoins spécifiques de certains clients. Ceci lui permet, entre autres, de réduire le risque relié aux systèmes de branchement différents de ses imprimantes dans les diverses régions du monde (11 OV versus 220V).

2.3.6. Le principe de précaution[3]

Une autre méthode de gestion du risque d'exploitation, mais cette fois-ci appliquée à l'environnement est basée sur *le principe de précaution* (Sylvie le Damany, Philippe Melot, Olivier Lantres, Elisabeth Minegier du Dorbier et Géraldine Brasier Porterie, 2000). Le principe apparaît en France au travers des dispositions de l'article L.200-1 du Code rural tel que modifié par la loi du 2 février 1995.

Cet article dispose que « *l'absence de certitudes, compte tenu des connaissances scientifiques et techniques du moment, ne doit pas retarder l'adoption de mesures effectives et proportionnées visant à prévenir un risque de dommages graves et irréversibles à l'environnement à un coût économiquement acceptable* ». Il entre en vigueur dans les différents pays principalement par le biais d'une nouvelle réglementation et a trouvé écho auprès de l'opinion publique notamment suite à l'apparition de certains sujets sensibles.

En fait ce principe théoriquement cantonné aux risques liés à l'environnement s'est retrouvé étendu à tous les problèmes d'ordre **alimentaire** ou liés aux sciences de la vie. Ce principe consiste en une politique préventive destinée à anticiper les risques et à mettre en place des mesures préventives visant l'évitement des risques qui nuissent à la communauté et à la société civile; il a pour rôle de responsabiliser les entreprises quant aux conséquences de leur exploitation sur l'environnement et éventuellement de les sanctionner en cas de manquement, à la condition, bien sûr, qu'une sanction soit prévue au niveau réglementaire.

[1] Olivier JENN; Op.cit. p78.
[2] Olivier JENN; Op.cit. p78.
[3] Idem ; Op.cit. P79.

3. Comparaison des méthodes et techniques d'analyse de risques

Il y a, sans doute autant de méthodes d'évaluation des risques qu'il y a des consultants, Nous avons retenu quelques unes qui ont fait l'objet d'une publication dont leur applicabilité, leur qualité, ainsi que leur pertinence sont différents.

3.1. Applicabilité des méthodes d'évaluation des risques

Le premier point de notre comparaison montre dans quelle mesure la technique s'applique à chaque étape du processus d'évaluation des risques, comme suit[1]:

- Identification du risque;
- Analyse du risque – analyse des conséquences;
- Analyse du risque – estimation de probabilité qualitative, semi-quantitative ou quantitative;
- Analyse du risque – évaluation du niveau de risque;
- Évaluation des risques.

Pour chaque étape du processus d'évaluation des risques, l'application de la méthode est présentées comme étant parfaitement applicable, applicable ou inapplicable (voir le tableau ci-dessous)

1 ISO/IEC 31010; Risk management-Risk Assessment Techniques ; p112.

Tableau N15°: Applicabilité des outils utilisés pour l'évaluation des risques

Outils et techniques	Processus d'évaluation des risques				
	Identification des risques	Analyse des risques			Evaluation des risques
		Conséquence	Probabilité	Niveau de risque	
« Brainstorming »	SA[1)]	NA[2)]	NA	NA	NA
Entretiens structurés ou semi-structurés	SA	NA	NA	NA	NA
Techniques Delphi	SA	NA	NA	NA	NA
Listes de contrôle	SA	NA	NA	NA	NA
Analyse préliminaire du danger	SA	NA	NA	NA	NA
Etudes de danger et d'exploitabilité (HAZOP)	SA	SA	A[3)]	A	A
HACCP[3]	SA	SA	NA	NA	SA
Evaluation des risques environnementaux	SA	SA	SA	SA	SA
SWIFT[4]	SA	SA	SA	SA	SA
Analyse de scénario	SA	SA	A	A	A
Analyse d'impact sur l'activité	A	SA	A	A	A
Analyse de causes profondes	NA	SA	SA	SA	SA
Analyse des modes de défaillance et de leurs effets	SA	SA	SA	SA	SA
Analyse par arbre de panne	A	NA	SA	A	A
Analyse par arbre d'événements	A	SA	A	A	NA
Analyse causes-conséquences	A	SA	SA	A	A
Analyse des causes et de leurs effets	SA	SA	NA	NA	NA
Analyse des niveaux de protection (LOPA)[5]	A	SA	A	A	NA
Arbre de décision	NA	SA	SA	A	A
Analyse de fiabilité humaine	SA	SA	SA	SA	A
Analyse «nœud papillon»	NA	A	SA	SA	A
Maintenance basée sur la fiabilité	SA	SA	SA	SA	SA
Analyse des conditions insidieuses (Analyse transitoire)	A	NA	NA	NA	NA
Analyse de Markov	A	SA	NA	NA	NA
Simulation de Monte-Carlo	NA	NA	NA	NA	SA
Analyse bayésienne et réseaux de Bayes	NA	SA	NA	NA	SA
Courbes FN	A	SA	SA	A	SA
Indices de risque	A	SA	SA	A	SA
Matrice conséquence/probabilité	SA	SA	SA	SA	A
Analyse coût/bénéfice	A	SA	A	A	A
Analyse de décision à critères multiples (ADCM)	A	SA	A	SA	A

Source: ISO/IEC 31010; Risk management-Risk Assessment Techniques ; p113.

3.2. Les critères de la qualité des méthodes d'évaluation des risques[1]

La qualité d'une analyse de risque doit être réévaluée au fur et à mesure de l'avancement d'un projet. Pour ce faire, nous proposons un ensemble de critères de la qualité des méthodes d'évaluation des risques comme suit:

3.2.1. Cohérence

La cohérence renvoie aux faits que :

- La démarche soit rationnelle et consensuelle.
- Les données et les résultats ne soient pas contradictoires, c.-à-d. qu'ils ne s'opposent ni entre eux ni avec les hypothèses de départ.

3.2.2. Complétude

La complétude peut être formalisée par les hypothèses suivantes:

- S'il existe un chemin causal inductif entre la cause A et la conséquence B, la cause A doit être déduite à partir de la conséquence B d'une façon immédiate ou différée (effet domino) suivant un chemin inverse déductif.
- Par analogie, pour tout chemin déductif, il doit y avoir un chemin inductif équivalent.

3.2.3. Exhaustivité

C'est la contrainte la plus difficile à satisfaire ou à démontrer, car l'analyste dans sa représentation de la réalité fait intervenir son intuition et son savoir-faire dans les limites de sa perception de cette réalité. Il peut donc porter un jugement disproportionné sur certains facteurs (cause, effet, probabilité, conséquence, etc.), comme il peut éventuellement manquer d'imagination par rapport à d'autres.

En effet, pour converger vers l'exhaustivité, il convient que l'analyse de risque soit :

- Élaborée au sein d'un groupe d'experts, idéalement en groupe pluridisciplinaire.
- Examinée par de tierces personnes externes.
- Assistée par des outils informatiques d'aide à la décision.

3.2.4. Intégrité

Assurance fournie par une organisation que l'analyse de risque est correctement accomplie à moins que les analystes, experts, ingénieurs ou autres, ne préviennent du manque de rigueur dans une quelconque étape, d'un désaccord sur un jugement, de la subjectivité dans l'estimation de paramètres telle que la probabilité d'occurrence, etc.

3.2.5. Traçabilité

L'analyse de risque n'est pas un but en soi, mais plutôt un moyen ayant pour but de démontrer le respect des exigences de sécurité. Chaque méthode est praticable dans un contexte particulier du cycle de vie d'un système. Chacune fait appel aux données disponibles et fournit un certain nombre de résultats qui devraient être repris, en tant que données d'entrée, par l'analyse suivante. Ainsi, de fil en aiguille, on se retrouve entrain de concevoir la partie management des risques du plan général de démonstration et de maintien de la sécurité en l'occurrence le SMS pour Safety Management System traduit en français par Système de Management de la Sécurité.

[1] Mohamed –Habib Mazouni; Op.cit. p 60.

3.3. Facteurs influençant le choix des techniques d'évaluation des risques [1]

Les attributs des méthodes sont décrits en terme de:

- Complexité du problème et méthodes nécessaires à son analyse;
- Nature et degré d'incertitude de l'évaluation des risques reposant sur la quantité d'informations disponibles et sur les éléments nécessaires à la satisfaction des objectifs;
- Étendue des ressources nécessaires en termes de durée et de niveau des expertises, de données nécessaires ou de coût;
- Possibilité pour la méthode de fournir des résultats quantitatifs.

Des exemples de types de méthodes d'évaluation des risques disponibles sont répertoriés dans le tableau N°16, dans lequel chaque méthode est classée selon que ses attributs sont élevés, moyen ou faibles.

Tableau N°16: Attributs d'un choix d'outils d'évaluation des risques

[1] ISO/IEC 31010; Risk management-Risk Assessment Techniques ; p115.

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
MÉTHODES DE RECHERCHE					
Listes de contrôle	Formulaire simple d'identification des risques. Technique proposant un répertoire d'incertitudes usuelles qu'il convient de prendre en compte. Les utilisateurs se rapportent à une liste, à des codes et à des normes préalablement établis	Faible	Faible	Faible	Non
Analyse préliminaire du danger	Une méthode d'analyse inductive simple consistant à identifier les dangers, ainsi que les situations et événements dangereux, pouvant nuire à une activité, une installation ou un système donné	Faible	Élevé	Moyen	Non
MÉTHODES DE SOUTIEN					
Entretien structuré et «brainstorming»	Moyen de rassembler un grand nombre d'idées et d'évaluations en les classant dans un groupe. Le «brainstorming» peut être stimulé par des invites ou par des techniques d'entretien en tête à tête ou seul contre tous	Faible	Faible	Faible	Non
Technique Delphi	Moyen permettant de combiner les avis d'un expert susceptibles de soutenir la source et d'avoir un impact sur l'identification, la probabilité et les conséquences et l'évaluation des risques. Il s'agit d'une technique collaborative permettant de prévoir un consensus. Implique l'analyse et le vote indépendants d'experts	Moyen	Moyen	Moyen	Non
Méthode ("que se passerait-il si ?")	Système incitant une équipe à identifier les risques. Il est en principe utilisé dans un atelier formel. En principe lié à une analyse des risques et une technique d'évaluation	Moyen	Moyen	Toutes	Non
Analyse de fiabilité humaine (AFH)	L'analyse de fiabilité humaine (AFH) porte sur l'impact des personnes sur les performances du système. Elle peut être utilisée pour évaluer les influences de l'erreur humaine sur le système	Moyen	Moyen	Moyen	Oui

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
ANALYSE DU SCÉNARIO					
Analyse de causes profondes (analyse la perte unique)	Une seule perte a été analysée afin de comprendre les causes concourantes et la manière dont le système ou le processus peut être amélioré pour éviter des pertes de ce type à l'avenir. L'analyse doit tenir compte des contrôles en place au moment de la perte et de la manière dont ils peuvent être améliorés	Moyen	Faible	Moyen	Non
Analyse du scénario	Les futurs scénarii possibles sont imaginés ou extrapolés à partir des risques actuels et différents considérés, en supposant que ces scénarii soient susceptibles de se produire. Il peut s'agir de scénarii formels ou informels, qualitatifs ou quantitatifs	Moyen	Élevé	Moyen	Non
Évaluation des risques toxicologiques	Les dangers sont identifiés et analysés, et les possibles vecteurs d'exposition au danger d'une cible spécifiée sont identifiés. Les informations relatives au niveau d'exposition et à la nature de la nuisance provoquée par un niveau d'exposition donné sont combinées pour donner une mesure de la probabilité d'occurrence de la nuisance spécifiée	Élevé	Élevé	Moyen	Oui
Analyse d'impact sur l'activité	Propose d'analyser la manière dont les principaux risques de perturbation pourraient avoir un impact sur les opérations d'une organisation et d'identifier et de quantifier les aptitudes nécessaires à leur gestion	Moyen	Moyen	Moyen	Non
Analyse par arbre de panne	Technique commençant par l'événement indésirable (événement de tête) et déterminant toutes les manières dont il pourrait se produire. Ces éléments sont présentés graphiquement sous la forme d'une arborescence logique. Une fois l'arbre de panne développé, il convient de considérer les manières de réduire ou d'éliminer les causes/sources potentielles	Élevé	Élevé	Moyen	Oui
Analyse par arbre d'événements	Utilisation du raisonnement inductif pour traduire la probabilité d'événements initiateurs différents en résultats possibles	Moyen	Moyen	Moyen	Oui
Analyse causes/ conséquences	Combinaison de l'analyse par arbre de panne et par arbre d'événements permettant d'inclure des actions différées. Les causes et les conséquences d'un événement initiateur sont considérées	Élevé	Moyen	Élevé	Oui
Analyse de cause à effet	Un effet peut avoir un certain nombre de facteurs contributifs pouvant être regroupés en différentes catégories. Les facteurs contributifs sont souvent identifiés par «brainstorming» et présentés sous forme d'arborescence ou de diagramme d'Ishikawa	Faible	Faible	Moyen	Non

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
ANALYSE FONCTIONNELLE					
AMDE et AMDEC	L'AMDE (Analyse des modes de défaillance et de leurs effets) est une technique qui permet d'identifier les modes et les mécanismes de défaillance, et leurs effets. Il existe plusieurs types de méthode AMDE: L'AMDE Conception (ou produit), qui est utilisée pour les composants ou les produits, l'AMDE Système utilisée pour les systèmes, l'AMDE Processus utilisée pour les processus de fabrication et d'assemblage, l'AMDE Service et l'AMDE Logiciel. L'AMDE peut être suivie d'une analyse de criticité qui définit l'importance de chaque mode de défaillance de manière qualitative, semi-qualitative ou quantitative (AMDEC). L'analyse de criticité peut se fonder sur la probabilité qu'un mode de défaillance donnera lieu à la défaillance du système, ou sur le niveau de risque associé au mode de défaillance, ou sur un degré de priorité du risque	Moyen	Moyen	Moyen	Oui
Maintenance basée sur la fiabilité	Une méthode permettant d'identifier les règles qu'il convient de mettre en place pour gérer les défaillances et atteindre de manière efficace et efficiente le niveau de sécurité, de disponibilité et d'économie requis du fonctionnement pour tous les types d'équipement	Moyen	Moyen	Moyen	Oui
Analyse transitoire (Analyse de conditions insidieuses)	Une méthodologie permettant d'identifier les erreurs de conception. Une condition insidieuse est une condition matérielle, logicielle ou intégrée latente pouvant être à l'origine d'un événement indésirable ou pouvant gêner l'occurrence d'un événement souhaité, cette condition n'étant pas provoquée par la défaillance d'un composant. Ces conditions se caractérisent par leur nature aléatoire et leur aptitude à échapper à toute forme de détection lors d'essais normalisés les plus rigoureux du système. Les conditions insidieuses peuvent être à l'origine de fonctionnements inappropriés, de la perte de disponibilité du système, de retards de programmation, voire de mort ou de blessure	Moyen	Moyen	Moyen	Non
Méthode HAZOP (Etudes de danger et d'exploitabilité)	Un processus général d'identification des risques permettant de définir les écarts possibles par rapport aux performances prévues ou attendues. Elle utilise un système reposant sur des mots-guides La criticité des écarts est évaluée	Moyen	Élevé	Élevé	Non
Méthode HACCP (Analyse des dangers critiques pour leur maîtrise)	Une méthode systématique, proactive et préventive visant à assurer la qualité des produits ainsi que la fiabilité et la sécurité des processus par la mesure et le contrôle de caractéristiques particulières devant se trouver dans des limites définies	Moyen	Moyen	Moyen	Non

Type de technique d'évaluation des risques	Description	Pertinence des facteurs influents			Résultat quantitatif
		Ressources et aptitudes	Nature et degré d'incertitude	Complexité	
ÉVALUATION DES CONTRÔLES					
Méthode LOPA (Analyse des niveaux de protection)	(Également appelée analyse de barrière). Elle permet d'évaluer les contrôles et leur efficacité	Moyen	Moyen	Moyen	Oui
Analyse «nœud papillon»	Un moyen schématique simple permettant de décrire et d'analyser les chemins d'un risque en partant des dangers jusqu'aux conséquences et en examinant les moyens de contrôle. Elle peut être considérée comme la combinaison d'un arbre de panne permettant d'analyser la cause d'un événement et d'un arbre d'événements permettant d'analyser les conséquences. Elle est représentée graphiquement sous la forme d'un "noeud papillon"	Moyen	Élevé	Moyen	Oui
MÉTHODES STATISTIQUES					
Analyse de Markov	L'analyse de Markov, parfois appelée analyse de l'*espace des états*, est habituellement utilisée dans l'analyse des systèmes complexes réparables qui peuvent exister en plusieurs états, notamment divers états dégradés	Elevé	Faible	Elevé	Oui
Analyse de Monte-Carlo	La simulation de Monte-Carlo permet d'établir la variation d'agrégat résultant des variations, dans un système, d'un certain nombre d'entrées, dont chacune d'elles est répartie de manière définie et est liée au résultat par des relations définies. L'analyse peut être utilisée pour un modèle spécifique, dans lequel les interactions des différentes entrées peuvent être définies mathématiquement. Les entrées peuvent reposer sur une variété de types de distribution, selon la nature de l'incertitude qu'elles sont censées représenter. Dans le cas de l'évaluation des risques, les distributions triangulaires ou distributions bêta sont souvent utilisées	Elevé	Faible	Elevé	Oui
Analyse bayésienne	Un mode opératoire statistique qui utilise les données d'une distribution préalable pour évaluer la probabilité du résultat. L'analyse bayésienne dépend de l'exactitude de la distribution préalable pour déduire un résultat exact. Le modèle de réseaux de croyance bayésienne a un impact dans une variété de domaines en capturant les relations de probabilité des entrées variables pour déduire un résultat	Elevé	Faible	Elevé	Oui

Source: ISO/IEC 31010; Risk management-Risk Assessment Techniques ; p115 -118.

Section 3 : Auditer l'efficacité du management du risque

Le management du risque est, parmi d'autres, un processus ou même une fonction de l'entreprise qui doit contribuer à l'amélioration de son efficacité pour ses clients, à la sécurité des hommes et de ses produits et à la rentabilité des fonds propres pour ses actionnaires.

A ce titre, comme toutes les autres fonctions/Processus de l'entreprise, le management du risque doit être audité pour confronter les dirigeants dans son l'efficients. Pour se faire, cette section est scindée en trois éléments, le premier expose les objectifs de l'audit de management du risque et les caractéristiques pour un système efficace de management du risque, ensuite nous allons présenter la revue de management du risque par l'audit interne, et nous finissons par l'assurance sur le processus de management du risque.

1. Les objectifs de l'Audit de management du risque et les caractéristiques pour un système efficace de management du risque

Le management du risque fait partie des fonctions ou des processus sensibles de l'entreprise. Il a accès à une quantité d'informations qui, si elles étaient utilisées à mauvais escient, pourraient déstabiliser gravement l'entreprise ; ce qui fait importe aux dirigeants de surveiller son bon exercice et fonctionnement de ce processus.

1.1. Les objectifs de l'Audit de management du risque

L'audit de management du risque, placé sous la responsabilité du président plutôt que du directeur générale, du conseil de surveillance plutôt que du directoire, doit permettre aux dirigeants, aux actionnaires et aux partenaires de l'entreprise de vérifier l'adéquation du processus de management du risque à la politique générale de management du risque définie par les dirigeants et validée par les administrateurs.

Les résultats de l'audit, sous forme de rapports au moins annuels, sont présentés aux dirigeants pour leur permettre de prendre, s'il y a lieu, les mesures correctrices nécessaires à l'amélioration de l'efficacité de management du risque au sein de l'entreprise. Le rapport annuel est naturellement complété et alimenté par des rapports spécifiques élaborés à l'occasion de chaque mission. L'audit interne et externe permet aussi de valider la qualité des informations publiées concernant le management du risque de l'entreprise.

Rappelons que, dans des grandes structures, il existe souvent, en appui de la Présidence, un comité d'audit qui étudie, au moins annuellement voire semestriellement, les résultats des travaux de vérification des activités de l'entreprise. Ceci fait l'objet d'un rapport d'audit général retraçant les conclusions des auditeurs.

Dons, les auditeurs doivent apprécier, de manière fiable, le dispositif de management du risque au même titre que toute autre processus de l'entreprise; cette fiabilité est assurée par leur indépendance par rapport au processus opérationnel, leur objectivité à partir du référentiel de management du risque, leur compétence en méthodologie et en compréhension des métiers et des activités audités.

Ils vérifient que[1]:

- La mise en œuvre de management du risque est conforme aux objectifs fixés par les dirigeants et précisés dans la politique générale de management du risque ;

- La fonction est rentable, c'est-à-dire exercée à un coût non disproportionné par rapport aux gains réalisés sur les coûts des risques ;

- Les mesures décidées pour réduire les risques sont opérationnelles (contrôle interne, contrôle qualité, plans de continuité d'activité. Etc.) ;

[1] Catherine Véret et Richard Mekouar; Fonction : Risk manager; Op.cit ; p220.

- Les traitements de financement des risques, particulièrement les programmes d'assurance souscrits, sont adaptés aux risques résiduels;

- Les outils mis en œuvre pour gérer les risques potentiels et avérés sont adéquats et fiables;

- Les reporting et tableaux de bord de management du risque reflètent «fidèlement» la réalité de l'entreprise et rendent compte de manière pertinente du suivi des risques.

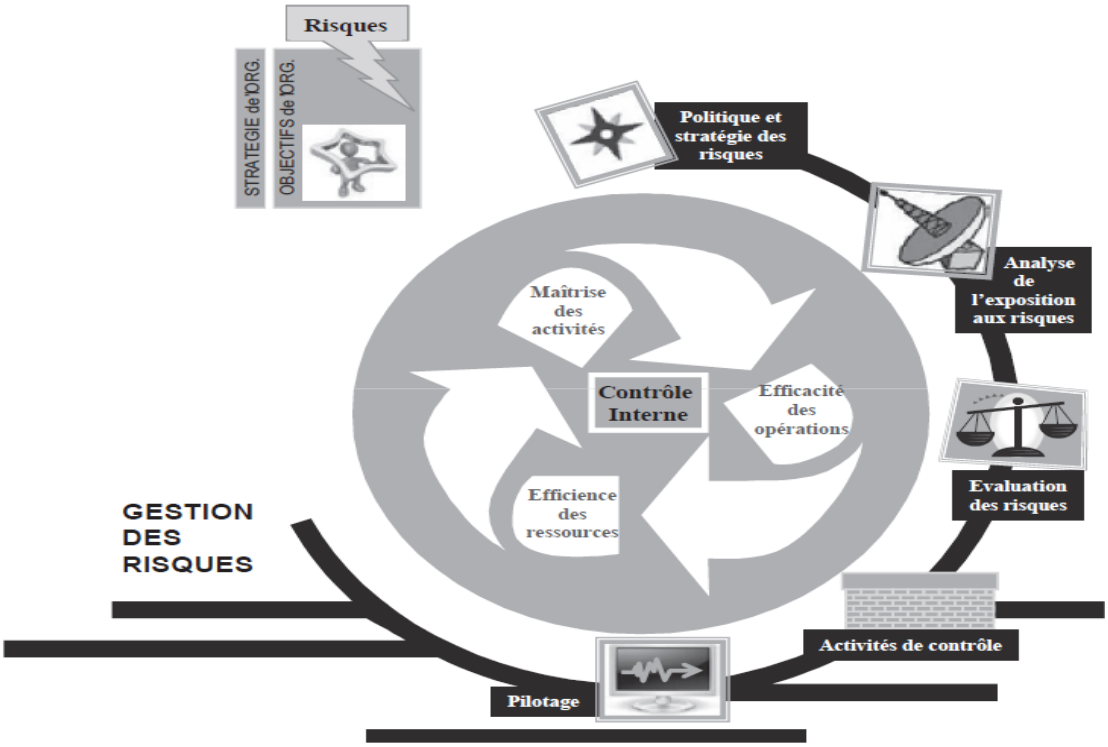
Ils s'assurent aussi qu'il n'y a pas de dérive inconnue ou cachée dans le processus de management du risque

L'audit du dispositif de management du risque ne doit pas se substituer au *Risk manager* lui-même, ce qui entraînerait une déperdition d'énergie pour l'entreprise. En ce sens, l'audit ne conçoit pas, ne met pas en œuvre les solutions pour diminuer les risques auxquels l'entreprise est exposée. L'audit contrôle que ces solutions existent et sont opérationnelles.

1.2. Les caractéristiques pour un système efficace de contrôle interne et de management du risque [1]

Un système est efficace dès lors qu'il répond aux objectifs pour lesquels il a été conçu et mis en œuvre. Ainsi, le système de management du risque et le processus de contrôle interne doivent fonctionner de manière imbriquée et coordonnée pour atteindre l'objectif de maîtrise des risques qui leur est assigné.

Figure N°47: Système de contrôle interne et de management du risque



Source: IFA & KPMG ; Gouvernance des risques et du contrôle : Quelle approche pour les comités d'audit? ; Les recontres de l'audit commitee institute; Institue Français des Administrateurs; 25 Novembre 2010 ; p22.

[1] IFA ; Le suivi de l'Efficacité des systèmes de contrôle interne et de gestion des risques; Guide Méthodologique; Institue Français des Administrateurs ; Novembre 2010; P6.

L'efficacité du système de management du risque et du contrôle interne passe par une bonne coordination des dispositifs autour d'activités-clés[1]:

- Cartographie et évaluation des risques ;
- Définitions et évaluation des activités de contrôle ;
- Plan de remédiation ;
- Pilotage et diffusion de l'information ;
- Supervision continue.

L'ensemble du dispositif doit être adapté aux caractéristiques propres de chaque entité. Néanmoins, quelle que soit l'organisation considérée, la mise en œuvre des 15 pratiques suivantes pourrait garantir l'efficacité du système [2]:

➲ **Politique et stratégie :**

1. L'appétence aux risques est définie par le conseil ;

2. Les responsabilités en matière de management du risque (y compris les problématiques de délégation) sont clairement définies et diffusées au sein de l'entité ;

➲ **Analyse de l'exposition aux risques :**

3. Le recensement des événements potentiels susceptibles d'avoir un impact sur les objectifs de la société est réalisé de manière exhaustive et l'univers des risques est régulièrement mis à jour ;

4. Les événements négatifs (internes/externes) pouvant générer des risques sont analysés ;

➲ **Évaluation des risques :**

5. Les risques et leurs incidences potentielles sont évalués ;

6. Les réponses aux risques sont élaborées ;

7. Les risques résiduels sont analysés en lien avec le niveau de risque acceptable tel que défini par le conseil ;

➲ **Activités de contrôle :**

8. Les activités de contrôle sont mises en œuvre dans chaque processus de l'organisation ;

9. Les activités de contrôle font l'objet d'une évaluation ou auto-évaluation ;

10. Les activités de contrôle sont supervisées par des fonctions de surveillance ;

11. L'évaluation des activités de contrôle fait l'objet d'une revue indépendante ;

➲ **Pilotage :**

12. Des indicateurs-clés de performance relatifs au dispositif de management du risque sont définis et suivis ;

13. Les plans de remédiation font l'objet d'un suivi documenté ;

14. Les incidents avérés sont recensés et analysés ;

15. Les objectifs et la stratégie du dispositif sont régulièrement mis à jour.

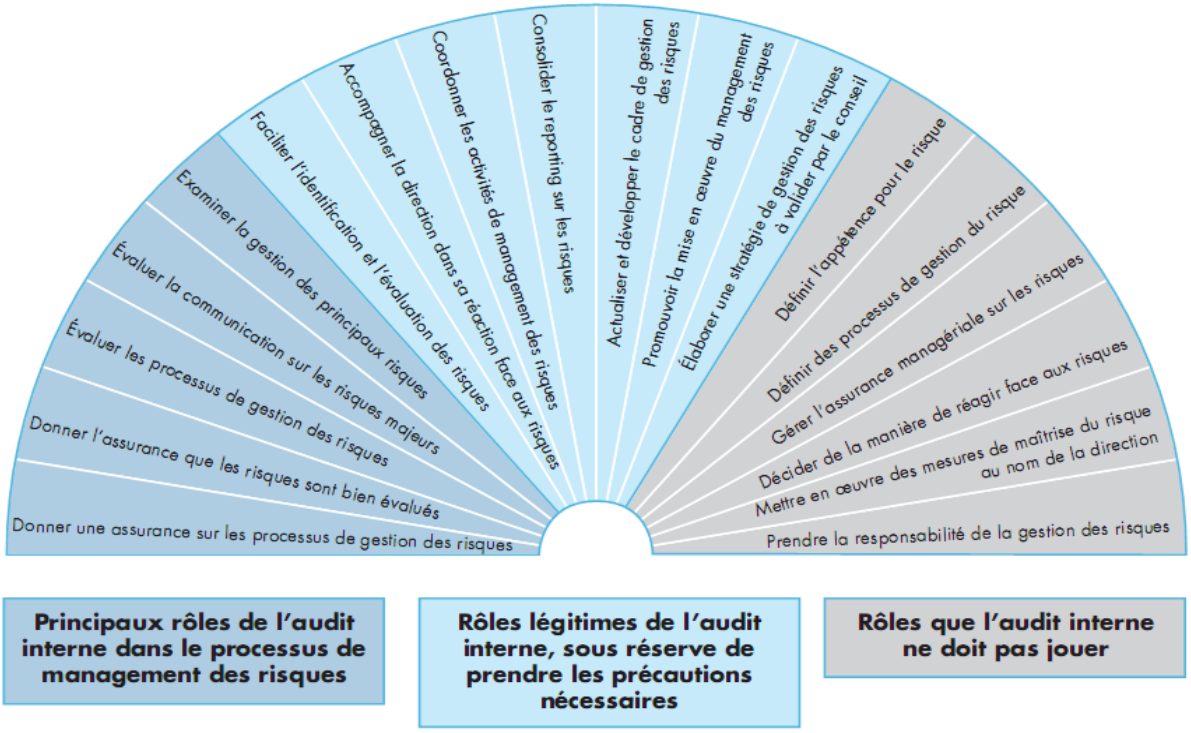
[1] IFA ; Le suivi de l'Efficacité des systèmes de contrôle interne et de gestion des risques; Novembre 2010; Op.cit ; p 5.
[2] IFA ; Le suivi de l'Efficacité des systèmes de contrôle interne et de gestion des risques; Novembre 2010; Op.cit ; p 6.

In fine, suivre l'efficacité d'un système revient à suivre le niveau de réalisation de ses objectifs. Cela suppose qu'il en existe une mesure, une évaluation.

2. La revue de management du risque par l'audit interne

Dans les domaines à risque les plus élevés, pour lesquels le management a admis la nécessité d'améliorer les contrôles, l'audit interne peut ajouter de la valeur par des activités de conseil. La partie centrale de la figure suivante présente les activités de conseil qui peuvent être fournies au niveau d'une entité ou d'une unité opérationnelle/d'un département en préservant l'indépendance et l'objectivité de l'audit interne.

Figure N°48 : Rôle de l'audit interne dans l'ERM



Source : IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p13.

2.1. Les activités d'assurance relatives au processus de management du risque

L'audit interne du processus de management du risque donne à la direction générale et au Conseil l'assurance raisonnable que le programme de management du risque est correctement conçu, documenté et mis en œuvre pour permettre la réalisation des objectifs de l'organisation. Cette assurance peut notamment permettre de répondre aux questions suivantes [1]:

- Le programme de management des risques bénéficie-t-il d'un engagement adéquat de la part du management de l'organisation, notamment d'un statut et de ressources en rapport avec les risques, et constitue-t-il une composante appropriée des processus organisationnels et de prise de décision ?

- La conception du cadre organisationnel de management du risque et les critères d'évaluation des risques sont-ils adaptés au contexte interne et externe de l'organisation ?

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Guide Pratique; Décembre 2010 ; p 14.

- Existe-t-il une définition et une communication adéquates des exigences, des critères d'évaluation des risques et des responsabilités concernant l'élaboration, la mise en œuvre et l'actualisation du cadre organisationnel de management des risques ainsi que des évaluations de domaines de risque spécifiques ?

- L'attitude face au risque est-elle décidée au niveau approprié dans la structure de gouvernance de l'organisation ?

- Les mécanismes de communication et d'information internes permettent-ils la diffusion appropriée des principaux résultats des activités relatives au management du risque au sein de l'organisation (en conciliant transparence et caractère sensible) ?

- Les rapports aux parties prenantes reflètent-ils de façon adéquate l'attitude de l'organisation face aux risques et leur traitement ?

- Les mécanismes de communication et d'information externes permettent-ils de se conformer à la législation, à la réglementation, aux principes de gouvernement d'entreprise et aux règles relatives à l'information des actionnaires ?

- Existe-t-il des mécanismes adéquats de mesure des performances et de remontée d'informations, permettant de surveiller la conception et l'efficacité du cadre organisationnel de management du risque ?

- Les critères d'évaluation des risques, le niveau d'appétence pour les risques, les réponses aux risques et la remontée de l'information sont-ils appliqués uniformément dans toute l'organisation ? Des personnes, disposant des connaissances appropriées, sont-elles responsables de l'identification des risques ? La maturité en matière d'identification des risques est-il adéquate ?

- Le cadre de management du risque ainsi que les processus et les contrôles associés sont-ils mis à jour lorsque les activités et les besoins organisationnels évoluent ?

- Les personnes responsables de l'analyse, de l'évaluation et du traitement /des réponses aux risques disposent-elles des connaissances appropriées ? Ces activités font-elles l'objet d'une revue et d'une validation adéquates ?

- Les plans de traitement des risques sont-ils suivis et communiqués de manière adéquate aux niveaux appropriés de la direction générale et du Conseil ?

2.2. Les activités d'assurance relatives aux risques significatifs et aux affirmations du management[1]

Pour tous les autres travaux d'assurance dont le périmètre concerne les risques de niveaux d'exposition importants (identifiés dans le cadre d'un processus de management du risque de l'organisation), les procédures et les communications de l'audit interne devraient être conçues pour évaluer les affirmations du management concernant l'efficacité des contrôles et leur capacité à réduire le risque à un niveau tolérable pour l'organisation.

Les rapports à la direction générale (et au Conseil) peuvent décrire l'exposition potentielle, et l'évaluation du management (y compris la qualité des contrôles en place) des risques actuels ainsi que l'évaluation des risques par l'audit interne. Chaque écart est pris en compte dans le processus de management des risques.

L'effet cumulatif des activités portant sur des domaines de risque spécifiques et réalisées dans le cadre d'un plan d'audit fondé sur les risques permettra de fournir une assurance non

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p 15.

seulement sur ces domaines de risque spécifiques mais également sur l'efficacité du processus global de management des risques.

2.3. Le suivi du plan de traitement des risques[1]

Dans le cas d'une exposition potentielle plus importante, il peut être approprié d'assurer le suivi de l'efficacité de la mise en œuvre des plans de traitement et de contrôle des risques, surtout si ces plans sont à long terme. Cette surveillance est, a minima, conçue pour communiquer au management une évaluation des avancées par rapport aux jalons définis et pour valider l'état d'avancement des plans de traitement des risques présentés au Conseil.

De plus, cette surveillance peut consister à évaluer la structure des plans, les ressources, les responsabilités, la gestion de projets, etc… Elle donne lieu à des recommandations et à des remarques visant à améliorer la probabilité de succès des plans.

2.4. Obtenir des preuves d'audit[2]

Concernant les audits du processus de management du risque d'une organisation, la Modalité pratique d'application 2120-1, Évaluer la pertinence des processus de management du risque, paragraphe 8, indique : « Afin de se forger une opinion sur l'adéquation des processus de management des risques, les auditeurs internes devront disposer d'éléments suffisamment probants et appropriés pour avoir l'assurance que les principaux objectifs de ces processus sont bien remplis. Pour recueillir ces éléments, l'auditeur interne peut recourir aux procédures d'audit décrites ci-après:

- Rechercher et analyser des informations sur le secteur d'activité de l'organisation, l'évolution récente et les tendances, ainsi que toute autre source d'information appropriée, afin de déterminer les risques susceptibles d'affecter l'organisation et les procédures de contrôle utilisées pour gérer, suivre et réévaluer ces risques ;

- Examiner les règles de l'entreprise ainsi que les procès-verbaux des délibérations du Conseil et du comité d'audit afin de déterminer les stratégies de l'organisation, son approche de management du risque, son appétence pour le risque et son acceptation des risques ;

- Examiner les rapports d'évaluation des risques précédemment établis par le management, les auditeurs internes ou externes et par tout autre intervenant ;

- Organiser des entretiens avec l'encadrement opérationnel et leur direction afin de déterminer les objectifs de chaque branche d'activité, les risques correspondants, et les mesures de suivi, de contrôle et d'atténuation des risques prises par le management ;

- Recueillir des informations afin d'évaluer, en toute indépendance, l'efficacité du processus de suivi, de communication et d'atténuation des risques, et des activités de contrôle correspondantes ;

- Déterminer si les informations ou rapports relatifs au suivi des risques sont adressés au niveau hiérarchique approprié ;

- Vérifier si les rapports concernant les résultats de management du risque sont diffusés selon des modalités et dans des délais appropriés ;

- S'assurer du caractère exhaustif de l'analyse des risques effectuée par le management et des mesures prises pour résoudre les points soulevés dans le cadre du processus de management du risque, et proposer des améliorations ;

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p 15.
[2] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p 16.

- Apprécier l'efficacité du processus d'auto-évaluation mis en œuvre par le management, au moyen d'observations et de tests sur les procédures de suivi et de contrôle testant l'exactitude des informations utilisées dans le cadre des opérations de suivi, et par d'autres techniques appropriées ;

- Examiner les signes de faiblesse éventuels du dispositif de management du risque et, le cas échéant, les analyser avec la direction générale et le Conseil. S'il estime que le management a accepté un niveau de risques non compatible avec la stratégie et les procédures de l'organisation en matière de management du risque, ou jugé inacceptable pour l'organisation, l'auditeur se réfèrera à la Norme 2600 relative à l'acceptation des risques par le management et aux lignes directives correspondantes pour des orientations complémentaires. »

Différentes techniques permettent d'obtenir des preuves d'audit, notamment[1] :

- Les observations, par exemple en étant présent lorsque des activités relatives au management du risque sont conduites aux différents échelons de l'organisation ; au niveau des organes dirigeants et jusqu'aux différents départements, programmes, projets et collaborateurs ;

- Les entretiens ;

- L'examen de documents, par exemple des ordres du jour, des documents de travail et des procès-verbaux, émanant notamment du conseil, de la direction générale et d'autres comités de la direction générale, des plans stratégiques ou des documents d'aide aux décisions relatives aux ressources ;

- Les résultats des audits antérieurs ;

- Les travaux réalisés par des tiers ;

- Les techniques analytiques, par exemple l'analyse causale (root cause analysis) des défaillances détectées ;

- La cartographie des processus ;

- L'analyse statistique, par exemple, l'analyse des types d'incidents ou de quasi-incidents (near-misses).

- L'analyse et l'évaluation des modèles de risques ;

- Les enquêtes ;

- L'analyse des auto-évaluations du contrôle interne.

Souvent, on utilisera une combinaison de plusieurs techniques d'audit afin de rassembler des informations et preuves d'audit suffisantes pour aboutir à une conclusion. L'auditeur choisit la procédure la mieux appropriée compte tenu de l'objectif de sa mission. Il détermine également si les ressources et les compétences requises sont disponibles pour effectuer tous les travaux nécessaires à l'obtention d'une opinion suffisamment étayée. Si tel n'est pas le cas, l'auditeur doit se demander s'il ne serait pas prudent soit de refuser d'exprimer une opinion, soit d'assortir cette opinion de réserves en excluant certains domaines ou risques de l'univers sur lequel porte l'opinion.

Les preuves d'audit nécessaires diffèrent suivant le type d'avis que l'auditeur souhaite rendre. C'est l'assurance affirmative qui apporte le niveau d'assurance le plus élevé et qui requiert également le plus de preuves d'audit pour étayer l'opinion. A titre d'exemple, une

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p 17.

telle opinion indique non seulement si les contrôles/processus d'atténuation des risques sont adéquats et efficaces, mais donne également une assurance raisonnable que, si des preuves du contraire existaient, elles auraient été identifiées.

L'assurance négative n'apporte pas un niveau d'assurance aussi important et ne nécessite donc pas autant de preuves d'audit. Lorsque l'auditeur rend une assurance négative, il affirme, par exemple, que, sur la base des travaux effectués, aucun point n'a attiré son attention. En rendant ce type d'opinion, l'auditeur n'endosse aucune responsabilité quant au caractère suffisant du champ et des procédures d'audit pour déceler tous les problèmes significatifs. Une telle opinion a généralement moins de valeur qu'une assurance positive.

Les conclusions d'audit doivent être factuelles, objectives et reposer sur des preuves d'audit suffisantes. Les preuves d'audit sont suffisantes lorsqu'elles sont documentées, adéquates et concluantes, de sorte qu'une personne prudente et informée pourrait parvenir aux mêmes conclusions que l'auditeur. Les preuves d'audit doivent être correctement documentées et organisées.

Le service d'audit ne doit pas donner, sans le savoir, de fausse assurance. La « fausse assurance » est un niveau de confiance ou d'assurance qui se fonde sur des perceptions ou des hypothèses plutôt que sur des faits.

Dans de nombreux cas, la simple intervention de l'audit interne dans un domaine peut aboutir à donner une fausse assurance. Le champ de la participation de l'audit interne peut être mal interprété et il peut s'en suivre une fausse assurance.

3. Assurance sur le processus de management du risque[1]

Un organe de direction doit être à même de déterminer dans quelle mesure le processus de management du risque en place dans son organisation répond aux besoins de cette dernière et respecte les bonnes pratiques généralement acceptées. Le management du risque étant une composante cruciale du dispositif de contrôle interne, une lacune dans les processus de management du risque indiquerait que le système de contrôle interne de l'organisation est déficient.

Il est important pour une organisation d'obtenir une assurance sur son processus de management du risque. Il faut que cette assurance tienne compte du fait que l'auditeur interne n'est peut-être pas indépendant de la fonction risk management. Dans ce cas, on pourra faire appel à une tierce partie pour obtenir une telle assurance.

Pour évaluer un processus de management du risque, on peut recourir aux trois formes d'assurance suivantes :

- Approche par les éléments du processus.
- Approche par les principes clés.
- Approche par le modèle de maturité.

Chaque approche se suffit à elle-même, mais chacune apporte une perspective différente sur l'efficacité d'un processus de management des risques dans une organisation. Souvent, c'est en retenant non pas une mais plusieurs approches que l'on obtient les résultats les plus riches d'enseignements et les plus utiles. Le processus de management des risques doit être défini en fonction de l'organisation, de sa taille, de sa culture, de ses objectifs et de son profil de risque. Par conséquent, le processus d'assurance doit lui aussi être défini en fonction des besoins de l'organisation.

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p 19.

Il convient de valider les résultats de toute analyse théorique en examinant si, en pratique, le cadre de management du risque fonctionne efficacement. Autrement dit, ce type d'activité d'assurance ne doit pas être mené isolément et doit toujours accompagner ou associer les activités classiques d'assurance fondée sur le contrôle :

- Si les risques sont efficacement identifiés et correctement analysés ;
- Si un traitement des risques et un contrôle adéquats et appropriés sont en place ;
- Si la direction procède à une surveillance et à un examen efficace pour détecter les changements dans les risques et les contrôles.

3.1. Approche par les éléments du processus[1]

Cette approche permet de vérifier que chaque élément du processus de management du risque est en place. Il est crucial de valider les intentions de la direction générale au moyen de preuves d'audit suffisantes pour confirmer que l'élément concerné est satisfaisant en pratique. Rares sont les cas où les seules affirmations du management pourraient être considérées comme suffisantes. La norme ISO 31000 identifie sept composantes du processus de management du risque :

✓ ***Élément 1 – Communication et concertation*** : Un management du risque sain nécessite une communication et une consultation structurées et régulières avec ceux qui sont concernés par les opérations de l'organisation et au sein du secteur d'activité.

✓ ***Élément 2 – Établissement du contexte*** : Il faut comprendre l'environnement externe (politique, social, etc.) et interne (objectifs, stratégies, structures, déontologie, discipline, etc.) de l'organisation ou de l'activité avant de pouvoir identifier toute la gamme des risques.

✓ ***Élément 3 – Identification du risque*** : L'identification des risques doit être un processus formel et structuré qui tient compte des sources de risque, des domaines d'impact, des événements ainsi que de leurs causes et conséquences potentielles.

✓ ***Élément 4 – Analyse du risque*** : L'organisation doit recourir à une technique formalisée pour prendre en compte les conséquences de chaque risque et leur probabilité de survenance.

✓ ***Élément 5 – Évaluation du risque*** : L'organisation dispose d'un mécanisme permettant de classer les risques en fonction de leur importance relative, de façon à déterminer l'ordre de priorité dans la mise en œuvre des traitements.

✓ ***Élément 6 – Traitement du risque*** : Un bon management du risque requiert des décisions rationnelles concernant le traitement des risques. Classiquement, ce traitement consiste à éviter l'activité qui induit le risque, à partager le risque, à maîtriser le risque au moyen de contrôles ou à accepter le risque et ne pas prendre de mesure supplémentaire.

✓ ***Élément 7 – Surveillance et revue*** : La surveillance consiste à vérifier l'avancement de la mise en œuvre des plans de traitement des risques, à surveiller les contrôles et leur efficacité, à s'assurer que les activités proscrites sont évitées et à vérifier que le contexte n'a pas évolué d'une façon qui a une incidence sur les risques.

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p19.

3.2. L'approche par les principes clés[1]

Cette approche repose sur l'idée que, pour être pleinement efficace, tout processus de management du risque doit respecter un minimum de principes ou de caractéristiques. La norme ISO 31000 y consacre un chapitre. Un audit reposant sur cette approche évalue dans quelle mesure ces principes se vérifient pour le processus de management du risque de l'organisation :

- **Le management du risque crée de la valeur et la préserve :** Il s'ensuit que plus la valeur en jeu est élevée, plus le management du risque doit être rigoureuse. Il s'ensuit également que l'organisation dispose de différentes techniques, correspondant à différents niveaux d'exposition.
- **Le management du risque est intégré aux processus organisationnels :** Le management du risque ne doit pas être perçu comme une tâche supplémentaire.
- **Le management du risque est intégré au processus de prise de décision :** Plus la décision est importante, plus ce lien doit être explicite.
- **Le management du risque traite explicitement de l'incertitude :** On attend des évaluations des risques qu'elles documentent les zones d'incertitude et déterminent comment remédier au mieux à l'incertitude identifiée.
- **Le management du risque est systématique, structuré et utilisé en temps utile ;**
- **Le management du risque s'appuie sur la meilleure information disponible :** L'obtention d'informations peut se révéler onéreuse et le processus doit donner des indications sur ce qui peut être considéré comme des informations suffisantes.
- **Le management du risque est adapté**. Il ne s'agit pas d'un processus prêt à l'emploi: il doit être adapté en fonction des activités de l'organisation.
- **Le management du risque prend en compte les facteurs humains et culturels**. Les processus doivent être adaptés à la compétence et à la culture des utilisateurs.
- **Le management du risque est transparent et participatif.** La participation adéquate et en temps opportun des parties prenantes est nécessaire.
- **Le management du risque est dynamique, itératif et réactif au changement**. Le processus doit être régulièrement examiné et adapté aux changements dans l'organisation et dans son environne- ment, de sorte qu'il reste pertinent.
- **Le management du risque facilite l'amélioration continue de l'organisme**. Le management du risque doit gagner en maturité parallèlement aux processus de l'organisation.

3.3. L'approche par le modèle de maturité[2]

L'approche par le modèle de maturité part du postulat de l'amélioration continue de la qualité de management du risque d'une organisation. Les systèmes de management du risque immatures ont un rendement très faible par rapport à l'investissement qui y a été consacré et sont souvent considérés comme des coûts de mise en conformité ou comme un poste obligatoire, qui vise davantage à rendre compte des risques qu'à y remédier efficacement. Les processus de management du risque efficaces sont construits progressivement, chaque étape du processus de maturité apportant une valeur additionnelle. L'approche par le modèle de maturité permet d'évaluer le processus de management du risque de l'organisation sur la

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p20-21.
[2] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p21.

courbe de maturité, de sorte que le Conseil et la direction générale peuvent juger s'il répond aux besoins de l'organisation et s'il se développe comme prévu.

Un aspect crucial de l'approche par le modèle de maturité est la mise en relation de la performance et des progrès du management du risque concernant l'avancement dans l'exécution du plan de management du risque, et d'un système de mesure et de management des performances. Les résultats ainsi obtenus peuvent être présentés à la direction générale et au Conseil comme des preuves de l'amélioration de management du risque. Un tel système se compose généralement des éléments suivants [1]:

- Des règles de fonctionnement, tenant compte des approches de management du risque en vigueur et anticipant les besoins stratégiques à venir. Les règles de fonctionnement s'appuient généralement sur une liste de d'exigences détaillées à l'aune desquelles tout progrès dans la mise en œuvre pourra être mesuré.
- Un guide sur la manière concrète de respecter les règles et les exigences associées.
- Un moyen de mesurer les performances effectives au regard de chaque règle et de chaque exigence.
- Un moyen d'enregistrer les performances et les progrès et d'en rendre compte.
- La vérification périodique indépendante de l'auto-évaluation effectuée par le management.

Les « principes » pratiques et essentiels détaillés dans l'ISO 31000 doivent constituer le point de départ de toute évaluation de la maturité. Ces principes s'intéressent non seulement à la question « cet élément du processus ou du système existe-t-il ? » mais ils permettent également de savoir si l'élément concerné est « efficace et pertinent pour l'organisation ? » et si l'élément concerné « est créateur de valeur ? ». En réalité, le principe fondamental est que le management du risque doit créer de la valeur.

L'évaluation des performances effectives est réalisée au regard de chaque règle de fonctionnement au moyen d'un système de mesure de la maturité en fonction des intentions, mais n'accorde la meilleure note que dans le cas d'une mise en œuvre complète et d'une application effective de la règle. Le tableau ci-dessous présente un modèle envisageable pour mesurer la maturité (d'après le concept original du Capability Maturity Model développé par la Carnegie Mellon University).

Tableau N°17: Modèle de maturité de management du risque

NIVEAU DE MATURITÉ	NUL	TRÈS FAIBLE	FAIBLE	BON	COMPLET
Signification	Très peu voire pas de conformité avec les exigences.	Une conformité limitée avec les exigences. Le management soutient le principe d'un management des risques, mais en pratique, l'application des règles est médiocre.	Conformité limitée à l'énoncé des éléments. Adhésion au principe mais conformité limitée en pratique.	Le management souscrit totalement au principe, mais, en pratique, la conformité n'est que partielle.	Conformité totale à l'énoncé des éléments- en principe et en pratique, à tout moment et partout.

Source : IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit; p22.

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; Décembre 2010 ; Op.cit ; p21.

3.4. Évaluer la qualité de la documentation portant sur le management du risque[1]

L'ampleur de la documentation de management du risque de l'entreprise (ERM) variera en fonction de la taille et de la complexité de l'entité. Les grandes organisations disposent généralement de manuels de procédures, de diagrammes formels, de descriptifs de postes, d'instructions opérationnelles, de diagrammes de flux des systèmes d'information, etc. Les organisations plus petites, moins complexes, disposent habituellement d'une documentation beaucoup plus restreinte.

De nombreux aspects de l'ERM peuvent être informels et ne pas être documentés, mais être néanmoins mis en œuvre régulièrement et être très efficaces. Ils peuvent être testés de la même manière que les activités documentées. Le fait que des éléments de l'ERM ne soient pas documentés ne signifie pas nécessairement qu'ils ne sont pas efficaces ou ne peuvent être évalués. Toutefois, un niveau adéquat de documentation rend la surveillance plus efficace, et présente aussi d'autres avantages : il permet aux collaborateurs de comprendre plus facilement le fonctionnement du processus et leurs rôles spécifiques, et simplifie la réalisation de modifications, si besoin est.

Pour décider de documenter le processus d'évaluation lui-même, l'auditeur interne s'appuiera généralement sur la documentation existante des processus de management du risque. Le plus souvent, la documentation existante sera complétée par des documents additionnels préparés par l'auditeur, notamment des preuves des tests et des analyses réalisés au cours du processus d'évaluation. La nature et l'ampleur de la documentation sont normalement plus importantes lorsque les affirmations concernant l'ERM sont destinées à d'autres parties.

Lorsque la direction générale se prononce, vis-à-vis de tiers, sur l'efficacité de l'ERM, elle devrait envisager de produire et de conserver une documentation étayant cette déclaration. L'auditeur interne devrait alors se demander :

- si une stratégie de gestion des informations sur les risques concerne toutes les sources d'informations possibles. et si cette stratégie est en place ;
- si les infrastructures nécessaires à la communication des informations sur les risques sont en place ;
- s'il existe des définitions communes ;
- s'il existe des recommandations concernant la création, la suppression et le partage des informations sur les risques ;
- si des ressources adéquates sont allouées ;
- si la technologie est rentable et utilisée à propos ;
- si la surveillance est proactive ;
- si les informations sur les risques sont intégrées dans le processus de planification ;
- si les informations sur les risques sont intégrées aux informations sur les performances.

Il convient de documenter ces éléments et toute décision visant à mettre en œuvre des activités/processus.

Cette documentation pourra se révéler utile si la déclaration concernée est, par la suite, remise en cause.

[1] IFACI & IIA; Évaluer l'Adéquation du management des risques; 2010 ; Op.cit; p23.

Conclusion

La cartographie des risques est un outil de maîtrise et de management qui prend tout son sens dans un environnement de plus en plus risqué pour les entreprises. C'est un outil de pilotage relativement explicite et visuel qui permet de situer les risques, de fixer des objectifs et de contrôler leur évolution.

La cartographie des risques donne une assurance supplémentaire à la maîtrise des activités d'entreprise, une bonne pratique adoptée par la plupart des entreprises dont les grands groupes, une démarche conforme avec l'ensemble des référentiels de management du risque.

La compréhension fine des métiers et de leurs processus, la clarté et la simplicité opérationnelle de la méthodologie, un savoir faire sur le calibrage et le pilotage de l'exercice, une grande rigueur dans la mise en œuvre et enfin une politique de communication et de formation, sont donc des conditions indispensables pour mettre en place une cartographie des risques permettant une identification et une évaluation exhaustive et homogène des risques majeurs susceptibles de remettre gravement en cause la poursuite de l'activité.

Cependant, cette vision simple de la cartographie peut être remplacée par une méthode plus sophistiquée de type « Scorecard » ou un chiffrage plus précis de la notation du risque qui s'insèrent dans le cadre des méthodes les plus répandues en matière d'évaluation des risques.

Méthodologiquement, entreprendre la démarche d'une cartographie des risques permet de parcourir une bonne partie du processus de management du risque: identifier, analyser, évaluer, hiérarchiser, traiter et suivre les risques.

Notant que le management du risque porte en interne sur les objets englobés par les critères « moyens », alors que le management du risque vis-à-vis de l'externe s'ordonne très facilement selon les critères « résultats ».

L'évaluation des risques commence par une activité de quantification ou de qualification des risques en déterminant l'amplitude de la probabilité d'occurrence et l'impact. Ce dernier est par définition l'évaluation de la conséquence du risque. Dans certains cas, une analyse de sensitivité accompagnera cette activité dans le but de calibrer les donnés.

Les méthodes semi-quantitatives utilisent des échelles d'évaluation numérique de probabilité et de conséquence et les combinent pour obtenir un niveau de risque grâce à une formule. Les échelles peuvent être linéaires ou logarithmiques ou faire l'objet d'autres relations, les formules utilisées pouvant également varier.

L'analyse quantitative estime les conséquences et la probabilité liées à des valeurs réalistes, produit des valeurs de niveau de risque dans des unités spécifiques définies lors du développement du contexte, définit le niveau de risque par des termes comme «élevé», «moyen» et «faible», ainsi qu'elle peut combiner conséquence et probabilité pour évaluer le niveau de risque qui en découle en fonction de critères qualitatifs. Il convient d'exprimer les niveaux de risque dans les termes les plus adaptés au type de risque et d'une manière facilitant l'évaluation des risques.

Dans certains cas, un risque peut être exprimé sous la forme d'une distribution de probabilité sur un ensemble de conséquences. Il n'est pas toujours possible ou souhaitable de procéder à une analyse quantitative complète en raison d'informations insuffisantes relatives au système ou à l'activité en cours d'analyse, du manque de données, de l'influence de facteurs humains, etc. ou parce que le résultat de l'analyse quantitative n'est pas garanti ou nécessaire.

Dans ces circonstances, il peut s'avérer judicieux de faire appel à des spécialistes reconnus dans leurs domaines respectifs pour procéder à un classement semi-quantitatif ou qualitatif, comparatif des risques. Même si une quantification exhaustive a été réalisée, il faut admettre

que tous les niveaux de risque calculés ne sont que des estimations. Il convient de veiller à s'assurer que leur niveau de précision et d'exactitude n'est pas incompatible avec la précision des données et méthodes d'analyse utilisées.

Les auditeurs internes et externes et les conseillers formulent régulièrement des recommandations visant à renforcer le management du risque. Les auditeurs porteront leur attention sur les principaux risques et les traitements y affèrent, ainsi que sur la conception des activités de contrôle. Des faiblesses potentielles peuvent être identifiées et des mesures alternatives recommandées à la direction, accompagnées d'informations utiles pour l'appréciation du rapport coût/bénéfices. Les auditeurs internes ou les collaborateurs réalisant des revues similaires peuvent contribuer au pilotage des activités d'une organisation de façon particulièrement efficace.