Macro-Cartographie des Risques par Audit: une méthode de diagnostic et de management global des risques d'entreprise

Alain Desroches, Sebastien Delmotte

Macro-Cartographie des Risques par Audit

Une méthode de diagnostic et de management global des risques d'entreprise

Alain Desroches
École centrale Paris,
Grande Voie des Vignes,
92295 Châtenay-Malabry cedex, France

Sébastien Delmotte
MAD-Environnement
15, rue du Laytié
31560 NAILLOUX

***Abstract*—Les risques perçus dans une activité d'entreprise, depuis la base jusqu'au plus haut niveau de la gouvernance, peuvent être considérés comme une photo instantanée des risques globaux perçus de l'entreprise. Chacun de ces risques impacte un ou plusieurs des processus ou fonctions de l'entreprise regroupés selon la norme ISO 9001 en trois grandes catégories : management, soutien et réalisation. La méthode de macro-cartographie des risques par audit s'inscrit dans la norme ISO 31000, et est fondée sur un processus d'analyse invariant dont les données d'entrées sont : (i) la cartographie des processus d'entreprise et la pondération de leur importance vue par la gouvernance ; (ii) le plan d'audit, construit avec la gouvernance, qui répartit le recueil de données sur les processus et sous-processus, dans les différents établissements de l'entreprise ; (iii) la construction des référentiels d'acceptabilité des risques au niveau des activités de base et au niveau de la gouvernance et des matrices de transfert qui les lient ; (iv) le recueil des perceptions des risques par des audits au niveau des activités des sous-processus et fonctions de base. Le traitement de ces données par les algorithmes de la méthode permet d'établir les cartographies des risques initiaux et résiduels à tous les niveaux de l'entreprise. La photographie des risques fournie est à la fois bottom-up, utilisant un premier référentiel d'acceptabilité des risques au niveau des activités, et top-down utilisant un second référentiel d'acceptabilité au niveau de la gouvernance. Ce diagnostic permet d'identifier les risques majeurs pour la gouvernance, et d'identifier les fonctions ou processus critiques qui demanderont une analyse des risques plus fine, comme l'AGR (Analyse Globale des Risques), pour la construction d'un plan de maîtrise des risques accompagné d'une analyse de son financement. Bien que nouvellement développée la macro-cartographie des risques par audit a par exemple été mise en œuvre au CNES (Centre National d'Etudes Spatiales) à la SHAM ou à l'EFS (Etablissement Français du Sang).**

***Index Terms*— cartographie des risques d'entreprise, gouvernance des risques, perception des risques, audit, risques majeurs**

I. Introduction

Le management global des risques est aujourd'hui un prérequis pour garantir les performances, la pérennité et la sécurité des activités (Entreprises, Projets) et des produits [1-5]. Devant l'augmentation de la complexité technique et organisationnelle des systèmes et l'émergence de risques nouveaux (environnements naturels, technologiques, sociaux-économiques, cybercriminalité…), il est indispensable d'aborder dans une même démarche les risques structurels, fonctionnels et conjoncturels et de fonder le processus de gouvernance des risques sur la définition d'un référentiel d'acceptabilité unique quel que soit le type de risque abordé. L'analyse des risques à la lumière d'un tel référentiel permet de les hiérarchiser et d'en déduire les risques majeurs afin de prioriser la mise en œuvre des actions de maîtrise. Lorsque le système est une entreprise de grande taille, dont l'organisation est fondée sur un nombre élevé de processus et de fonctions qui peuvent de surcroît être distribuées géographiquement, l'application en première approche des méthodes inductives d'analyse fine des risques comme l'AGR (Analyse Globale des Risques) [1] deviennent dispendieuses en ressources humaines et financières. Préalablement, il est avantageux d'établir un premier diagnostic en mettant en œuvre la macro-cartographie des risques par audit. Cette méthode est fondée sur le recueil de la perception des risques au niveau des activités de base, puis son transfert aux niveaux supérieurs d'organisation et son évaluation dans le référentiel d'acceptabilité des risques de la gouvernance de l'entreprise. Rapide et facile à mettre en œuvre à grande échelle, la méthode permet de cartographier les risques perçus à tous les niveaux de l'entreprise (Fig. 1), fournissant les éléments de décision relatifs aux risques stratégiques majeurs. Elle répond au standard de l'ISO31000 [6].

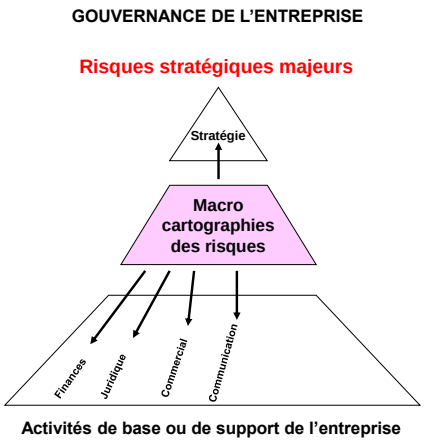

Fig. 1. Elaboration de la cartographie des risques

II. CONCEPTS PRELIMINAIRES

Le danger dont la notion précède celle de risque est défini comme un potentiel de préjudice ou de nuisance aux

personnes, aux biens ou à l'environnement. Ce concept abstrait couvre aussi bien des éventualités physiques ou matérielles accessibles par nos sens que des éventualités immatérielles comme l'énergie potentielle ou cinétique. De façon plus générale, un danger peut être une substance (produit toxique. . .), un objet (virus, astéroïde…), un phénomène (inondation, séisme, changement climatique, réaction exothermique. .) ou un processus (erreur de diagnostic, erreur de décision. . .). Ce préliminaire étant fait, le risque met en jeu deux notions. L'une, qualitative qui concerne son origine, à savoir l'exposition du système au danger, appelée situation dangereuse, qui, suivant les circonstances, peut se transformer en événement redouté avec des conséquences de différentes natures et importances. L'autre, quantitative qui est la « mesure » en termes de probabilité et de gravité de l'incertitude de la situation dangereuse ou de l'événement redouté. Si sur une échelle de temps, l'événement redouté est considéré à l'instant présent, alors sa probabilité d'occurrence concerne ses causes qui appartiennent à son passé tandis que la gravité concerne ses conséquences qui appartiennent à son futur.

Le risque d'un événement est un concept abstrait qui nécessite donc de prendre en compte de façon globale son passé, son présent et son futur. Il en résulte que le couple « probabilité–gravité » est indissociable et doit être considéré comme une variable bidimensionnelle.

Par-là même un risque n'est ni une probabilité, ni une gravité, mais les deux en même temps. Il s'ensuit qu'une décision associée à un risque ne peut être prise sur la base d'une seule de ses deux composantes. De sa nature bidimensionnelle, pour laquelle il n'existe pas de relation d'ordre, il découle que l'on ne peut hiérarchiser formellement deux risques de façon directe par le couple gravité–probabilité.

Dans la pratique, l'identification des risques est faite en utilisant un ensemble d'outils méthodologiques traitant de façon complémentaire de la nature des événements et de leurs localisations spatiale et temporelle. L'évaluation des risques est faite, d'une part, sur l'incertitude de l'occurrence en utilisant soit une échelle d'index de vraisemblance (analyse qualitative ou semi-quantitative) ou de valeurs de probabilité (analyse quantitative) et, d'autre part, sur les conséquences en utilisant une échelle d'index de gravité ou de valeurs de pertes et d'efforts. La maîtrise des risques est associée directement aux actions de réduction et de contrôle faites sur les composantes du risque : la prévention regroupe les actions qui ont pour but de diminuer la probabilité d'occurrence du risque tandis que la protection regroupe les actions qui ont pour but de diminuer la gravité des conséquences.

Le processus de réduction des risques est basé sur le concept de criticité du risque qui ne peut être mis en œuvre que lorsque la gouvernance du risque a préalablement fait la répartition de l'ensemble des risques de l'activité en trois zones correspondant à leur criticité suivant le principe ALARA (As Low As Reasonably Achievable), à savoir en :

- risque acceptable en l'état ;
- risque tolérable sous contrôle ;
- risque inacceptable.

L'ensemble de ces zones est visualisé respectivement en vert, jaune et rouge sur la Fig. 2.

La criticité du risque, est le résultat d'une fonction de décision associée à une échelle de valeurs politique, éthique, religieuse, économique, qui pour chaque risque évalué associe ou non une action de réduction ou de contrôle. La criticité du risque ne doit pas être confondue avec le risque moyen qui est le produit de la probabilité par la gravité du risque et n'est qu'un paramètre d'évaluation et non de décision.

Enfin, à la notion d'acceptabilité du risque s'ajoute celle du financement du risque. Il est fondé :

- d'une part sur l'évaluation du bénéfice/risque, c'est-à-dire le rapport des gains potentiel liés à la présence d'une opportunité par rapport aux pertes potentielles liées à la présence d'un danger. Une telle évaluation nécessite d'aborder conjointement pour un même système l'analyse des risques positifs et l'analyse des risques négatifs ;
- d'autre part sur l'évaluation des pertes/risque, c'est-à-dire le rapport des pertes attendues si on ne fait rien et des coûts liés à la mise en œuvre d'actions de réduction des risques. La décision de traitement du risque est politique si les coûts sont supérieurs aux pertes et économiques si les pertes sont supérieures aux coûts.

Classe de criticité	Intitulé de la classe	Intitulés des décisions et des actions
C1	Acceptable	Aucune action n'est à entreprendre
C2	Tolérable sous contrôle	On doit organiser un suivi en termes de gestion du risque
C3	Inacceptable	On doit refuser la situation et prendre des mesures en réduction des risques sinon … on doit refuser toute ou partie de l'activité

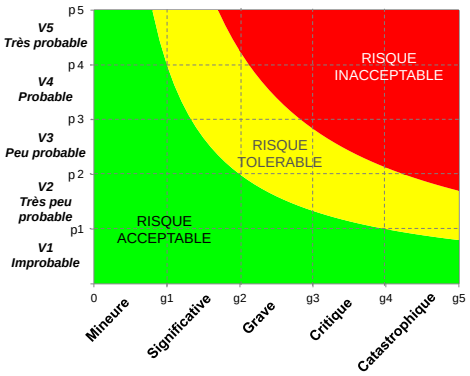

Fig. 2. Diagramme d'acceptabilité des risques (Farmer) et échelle de criticité et de décisions associées

Une troisième composante du risque peut être introduite : c'est la perception du risque. Elle est définie par l'appréciation subjective de la gravité ou de la probabilité alors appelée vraisemblance du risque.

Les risques perçus dans une activité d'entreprise, depuis la base jusqu'au plus haut niveau de la gouvernance, peuvent être considérés comme une photo instantanée des risques globaux perçus de l'entreprise. C'est sur ce principe que se fonde la macro-cartographie des risques par audit.

III. PRINCIPES ET METHODES

A. Cartographie des processus d'entreprise et logique des évaluations des risques

Dans la suite de cet article, le terme « système » fait référence aux caractéristiques de l'entreprise dans sa globalité. Le terme « processus » couvre les trois classes « management » (M), « réalisation » (R) et soutien (S). La figure 3 présente un exemple de cartographie des processus d'entreprise regroupés selon cette typologie issue de la norme ISO9001 [7]. Le terme « sous-processus » fait référence à l'une des composantes des processus, par exemple M1 ou M2. Le terme « activité » désigne des entités fonctionnelles ou opérationnelles de l'entreprise, opérant sur le même site ou des sites différents et pouvant être, pout tout ou partie, impliquée dans un sous-processus.

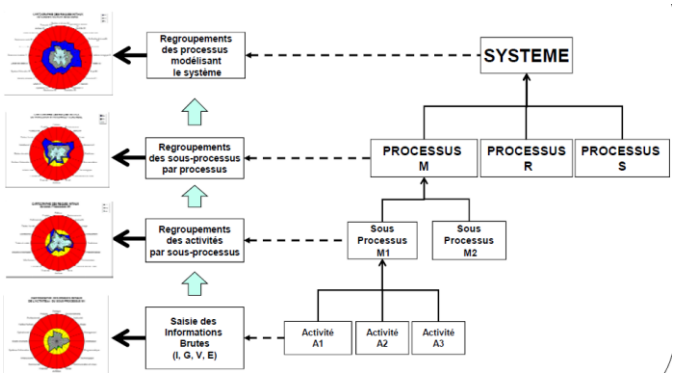

Fig. 3. Hiérarchisation des activités, sous-processus et processus dans le système et logique d'évaluation.

Cette terminologie traduit la hiérarchisation du système « Entreprise » illustrée par la figure 3. La logique d'évaluation des risques est fondée sur le transfert et le regroupement successif des risques perçus des activités aux niveaux supérieurs de l'organisation jusqu'au niveau global du système, pour en fournir la cartographie des risques.

B. Dangers d'entreprise

La cartographie des dangers, liste structurée de dangers, est élaborée à partir d'une liste de 26 dangers génériques qui couvre les catégories suivantes, détaillés dans le tableau 1 : dangers externes au système ; dangers de gouvernance du système ; dangers liés aux moyens techniques du système ; dangers liés aux études et à la production du système

TABLEAU 1. Typologie des dangers d'entreprise

Externes	Internes liés à la gouvernance	Internes liés aux moyens techniques	Internes liés à la production
Environnements	Commercial	Infrastructures et locaux	Etudes et projets
Politique	Communication et crises	Matériels et équipement	Opérationnel
Insécurité	Economique	Système d'information	Fonctionnel
Image	Entreprise		Facteur humain
Client	Ethique		Professionnel
	Financier		Produit
	Juridique		Physico-chimique
	Management		*Clinique*
	Programmatique		
	Social		
	Stratégique		
	Technologique		

C. Plan d'audit et supports d'audit

Le plan d'audit est défini avec et validé par la gouvernance du système (Tableau 2). Des pondérations des activités et des processus (donc des audits) peuvent être introduites par la gouvernance pour être appliquées lors de la cartographie des risques au niveau du système.

TABLEAU 2. Exemple de plan d'audit

			Structure et activités de l'entreprise															Nombre total d'activités auditées	
			Siège			Etablissement A					Etablissement B				Etablissement C				
Processus	Sous-processus	Abrév	A1/S	A2/S	A3/S	A1/A	A2/A	A3/A	A4/A	A5/A	A1/B	A2/B	A3/B	A4/B	A1/C	A2/C	A3/C		
Management (M)	Décision et organisation	M1	1	1														2	11
	Elaboration stratégie	M2	1	1														2	
	Programmation	M3	1	1														2	
	Maîtrise de la Qualité	M4	1	1	1													3	
	Prospective	M5		1	1													2	
Réalisation (R)	R&T	R1				1					1				1			3	21
	Avant projets	R2							1		1							2	
	Projets	R3					1								1			2	
	Opérations	R4					1				1							2	
	Collecte	R5					1				1							2	
	Préparation	R6					1										1	2	
	QBD	R7					1							1				2	
	Approvisionnements	R8				1									1			2	
	Distribution	R9				1					1							2	
	Biothèque	R10						1									1	2	
Soutien ou support (S)	Achats	S1			1					1				1			1	4	24
	Ventes	S2							1							1		2	
	Maîtrise de l'information	S3			1			1										2	
	Sécurité du travail	S4							1				1			1		3	
	Ressources humaines	S5			1			1						1		1		4	
	Ressources financières	S6		1														1	
	Sûreté et protection	S7			1					1								2	
	Communication externe	S8	1			1												2	
	Juridique	S9	1			1												2	
	Contrôle qualité	S10								1				1				2	

Les audits sont menés auprès des responsables d'activité, c'est-à-dire des personnes qui ont à la fois une bonne connaissance de l'activité et qui en ont la responsabilité du bon déroulement. Les audits peuvent être multipliés pour une même activité, particulièrement si elle est réalisée sur plusieurs sites. Cette multiplication permet d'évaluer la dispersion des valeurs des paramètres enregistrés et de tenir des spécificités locales d'une activité si elle est distribuée géographiquement.

Les audits sont menés en utilisant à la fois un questionnaire ouvert et un support de recueil des données de perception (Tableau 3). Le questionnaire ouvert permet d'évaluer la connaissance qu'a le responsable audité de l'activité ainsi que la maturité de la gestion des risques en place. Ces informations sont utiles pour interpréter les résultats finaux et pour initier ultérieurement des analyses de risques plus fines.

TABLEAU 3. Exemple de support d'audit de recueil des données

N°	Dangers génériques de l'activité d'entreprise		I	G	V	E
1	Dangers externes à l'activité de l'entreprise	Politique				
2		Environnements				
3		Insécurité				
4		Image				
5		Client				
6	Dangers liés à la gouvernance de l'entreprise	Entreprise				
7		Management				
8		Stratégique				
9		Programmatique				
10		Technologique				
11		Communication et crises				
12		Social				
13		Ethique				
14		Juridique				
15		Financier				
16		Economique				
17		Commercial				
18	Dangers liés aux moyens techniques de l'entreprise	Infrastructures et locaux				
19		Matériels et équipements				
20		Système d'information				
21	Dangers liés aux études et à la production de l'entreprise	Etudes et projets				
22		Opérationnel				
23		Facteur humain				
24		Professionnel				
25		Physico-chimique				
26		Produits				

D. Paramètres d'évaluation et de décisions des activités et des processus

Aux niveaux « Activités », « Sous-processus », « Processus », ou « Système », la perception et l'acceptabilité des risques peuvent être différentes. Il faut donc définir des échelles de gravité et de vraisemblances spécifiques pour l'activité et pour l'un des trois autres niveaux, appelé « niveau supérieur » (à définir en fonction des objectifs de l'étude) avec une fonction de transfert de l'activité à ce niveau pour ces deux paramètres d'évaluation. Il existe un référentiel d'acceptabilité des risques spécifiques pour chacun des deux niveaux.

1) Niveau de l'activité

Le facteur d'importance caractérise la perception de l'importance de l'activité sur le niveau supérieur par le responsable de l'activité (et non par la gouvernance). L'échelle du facteur d'importance est présentée dans le tableau 4.

TABLEAU 4. Echelle du facteur d'importance

Classe	Intitulé	Nature des conséquences perçues	Index d'importance (I)
I0	Nulle	Les résultats de l'activité n'ont *aucun impact* sur ceux du processus associé et du système	0
I1	Insignifiante	Les résultats de l'activité ont un *impact insignifiant* sur ceux du processus associé et du système (AD)	1
I2	Faible	Les résultats de l'activité ont un *impact faible* sur ceux du processus associé et du système (AD)	2
I3	Moyenne	Les résultats de l'activité ont un *impact moyen* sur ceux du processus associé et du système (AD)	3
I4	Forte	Les résultats de l'activité ont un *impact fort* sur ceux du processus associé et du système (AD)	4
I5	Très forte à totale	Les résultats de l'activité ont un *impact très fort* sur ceux du processus associé et du système (AD)	5

La gravité caractérise la perception du préjudice, du dommage ou de la perte. L'échelle associée est structurée en 5 niveaux chacun associé à la description de la nature des conséquences (Tableau 5)

TABLEAU 5. Echelle de gravité

Classe	Intitulé	Nature des conséquences	Index de Gravité
G1	Mineure	Aucune conséquence sur la performance ou l'intégrité de l'activité ou du système	1
G2	Significative	Des objectifs de l'activité ou du système n'ont pas été atteints	2
G3	Grave	Aucun des objectifs de l'activité ou du système n'a été atteint	3
G4	Critique	Mise en difficulté ou dégradation de l'activité ou du système	4
G5	Catastrophique	Perte totale de l'intégrité ou disparition de l'activité ou du système	5

La vraisemblance caractérise la perception de l'occurrence du préjudice, du dommage ou de la perte. L'échelle de vraisemblance est structurée en 5 niveaux qui peuvent associés à une période de retour (Tableau 6).

TABLEAU 6. Echelle de vraisemblance

Classe de vraisemblance	Intitulé	Index de vraisemblance
V1	Extrêmement improbable	1
V2	Très peu probable	2
V3	Peu probable	3
V4	Probable	4
V5	Probable à certain	5

La criticité caractérise la perception du risque de l'activité (gravité, vraisemblance) relativement à une échelle de valeurs. Elle est structurée en 3 niveaux d'acceptabilité chacun associé à une décision (Tableau 7).

TABLEAU 7. Echelle de criticité

Classes de criticité	Niveau du risque	Décision associée
C1	Acceptable en l'état	Aucune action n'est à entreprendre
C2	Acceptable sous contrôle	On doit organiser un suivi en termes de gestion du risque dont son transfert par la prise d'assurance
C3	Inacceptable	On doit refuser la situation et prendre des mesures en réduction des risques Sinon refuser de toute ou partie de l'activité

Le référentiel d'acceptabilité ou tableau de criticité caractérise les niveaux d'acceptation des risques (G_A, V_A) pour l'activité (Tableau 8).

TABLEAU 8. Exemple d'échelle de criticité au niveau « Activités »

		Gravité				
		1	**2**	**3**	**4**	**5**
Vraisemblance	**5**	1	2	3	3	3
	4	1	2	3	3	3
	3	1	1	2	3	3
	2	1	1	2	2	3
	1	1	1	1	2	2

L'effort caractérise les moyens et investissements perçus comme nécessaires pour maîtriser le risque (Tableau 9).

TABLEAU 9. Echelle d'effort

Classes	Niveau	Commentaires	Index
E0	Aucun	Aucune action entreprise	0
E1	Faible	Effort très faible à faible (e.g. coûts>,…) Vigilance, contrôle ou action ponctuel	1
E2	Moyen	Effort moyen (e.g. coûts>,…) Vigilance, contrôle ou action périodique	2
E3	Fort	Effort important à très important (e.g. coûts>,…) Vigilance, contrôle ou action continue Action au plus haut niveau	3

2) Fonctions de transfert des gravités et vraisemblances des Activités à celles des Sous-processus, des Processus ou du Système

Ces fonctions définissent les valeurs de gravité et de vraisemblance au « niveau supérieur » de l'activité (sous-processus, processus ou système) en fonction du facteur d'importance (Fig. 10).

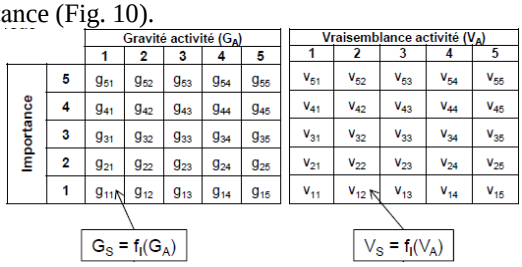

Fig. 10. Fonctions de transfert de la gravité et la vraisemblance entre le niveau « Activités » et le niveau supérieur (Sous-processus, Processus ou Système)

Elles traduisent le fait qu'un risque peut par exemple être perçu comme ayant des conséquences critiques au niveau de l'activité alors qu'elles seront seulement jugées graves au niveau du système si l'activité a une importance faible pour celui-ci. A l'inverse, les conséquences pourront être perçues comme graves au niveau de l'activité alors qu'elles seront considérées comme critiques au niveau du système, si l'activité a une importance très forte pour celui-ci.

3) Niveau du Sous-processus, du Processus ou du Système

La criticité caractérise la perception du risque (gravité, vraisemblance) au niveau sous-processus, processus ou système relativement à une échelle de valeur.

Le tableau de criticité caractérise les niveaux d'acceptation des risques (G_S, V_S) pour les sous-processus, processus ou système.

TABLEAU 10. Exemple d'échelle de criticité au niveau supérieur (Système, Processus ou Sous-processus)

Vraisemblance \ Gravité	1	2	3	4	5
5	1	2	3	3	3
4	1	2	2	3	3
3	1	1	2	3	3
2	1	1	2	2	3
1	1	1	1	2	2

E. Logigramme d'évaluation de la perception des risques (Figures 11 et 12)

Les risques perçus (G_A, V_A) de l'activité sont d'abord transférés au « niveau supérieur » en utilisant les fonctions de transferts $G_S=f_I(G_A)$ et $V_S=f_I(V_A)$. Leur criticité est ensuite évaluée à l'aune du référentiel de criticité du niveau « activité », fournissant la cartographie des risques initiaux des activités. L'algorithme de réduction des risques initiaux en fonction des efforts perçus fournit les risques résiduels des activités.

Ces risques initiaux et résiduels des activités sont ensuite regroupés par sous-processus et leur criticité est évaluée en utilisant :

- le référentiel d'acceptabilité du niveau « Activités » si le niveau évalué est inférieur au « niveau supérieur » choisi ;
- le référentiel d'acceptabilité du niveau « Supérieur » si le niveau évalué est le même ou est supérieur au « niveau supérieur » choisi.

On obtient ainsi les cartographies des risques au niveau sous-processus. Le même processus de regroupement formalisé est appliqué au niveau des processus, puis au niveau du système.

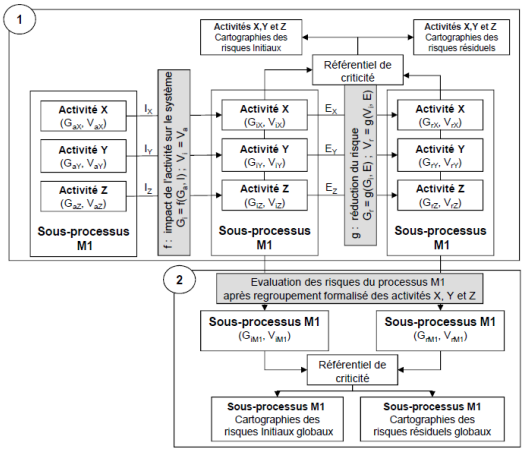

Fig. 11. Processus d'évaluation et de cartographie des risques initiaux et résiduels. Etapes 1 et 2.

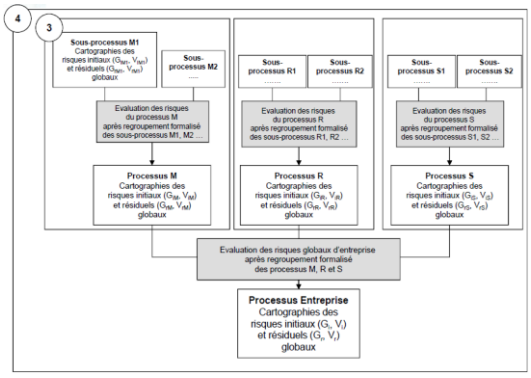

Fig. 12. Processus d'évaluation et de cartographie des risques initiaux et résiduels. Etapes 3 et 4.

En suivant ce processus d'évaluation, il en vient que :

- si le « niveau supérieur » est le Système, alors les risques évalués sont les risques des activités ayant un impact sur le système. Les risques aux niveaux Activités, Sous-processus et Processus sont évalués avec le référentiel d'acceptabilité « Activités » (vision bottom-up) ; les risques au niveau Système sont évalués avec le référentiel d'acceptabilité « Système » (vision top-down).
- si le « niveau supérieur » est le Processus, alors les risques évalués sont les risques des activités ayant un impact sur les processus. Les risques aux niveaux « Activités » et « Sous-processus » sont évalués avec le référentiel d'acceptabilité « Activités » (vision bottom-up) ; les risques aux niveaux système et processus sont évalués avec le référentiel d'acceptabilité « Processus » (vision top-down).
- si le « niveau supérieur » est le Sous-processus, alors les risques évalués seront les risques des activités ayant un impact sur les sous-processus. Les risques au niveau « Activités » sont évalués avec le référentiel d'acceptabilité « Activités » (vision bottom-up) ; les risques aux niveaux Système, Processus et Sous-processus sont évalués avec le référentiel d'acceptabilité « Sous-processus » (vision top-down).

IV. Exemples de resultats

A. Cartographie globale des risques

Les valeurs maximale, moyenne et minimale des risques moyens ($G_S \times V_S$) par activités sont projetées dans le tableau initial du plan d'audit (Tableau 11). Cette cartographie globale offre une vision synthétique des risques par activités distribuées géographiquement. Son analyse permet notamment de détecter des dysfonctionnements spécifiques à certains établissements, mais aussi de questionner les données de certains audits qui pourraient se distinguer par des résultats « anormaux » de valeurs de risques.

B. Cartographies des risques initiaux et résiduels

Au niveau du système, les cartographies des risques se déclinent :

- par processus, sous formes de diagrammes de Kiviat (Fig. 13) ou de Farmer (non représenté) ;
- par sous-processus (diagrammes de Kiviat en Fig. 13 et de Farmer en Fig. 14). Les efforts perçus pour réduire les risques initiaux sont également cartographiés par sous-processus ;
- par cibles d'impact (Fig. 16), définies par regroupement des sous-processus en 5 catégories de cibles: Techniques, Financières, Humaines, Management, Environnements ;
- par dangers génériques (Fig. 17) et par catégories de dangers d'entreprise (Fig. 18)

Ces cartographies des risques sont également réalisées à chaque niveau hiérarchique du système, c'est-à-dire au niveau des processus, des sous-processus et des activités (Figure 18).

TABLEAU 11. Projection des valeurs maximales des risques moyens ($G_S \times V_S$) par activités dans le tableau du plan d'audit

Risques moyens maximum			Structure et activités de l'entreprise														
			Siège			Etablissement A					Etablissement B				Etablissement C		
Processus	Sous-processus	Abrév	A1/S	A2/S	A3/S	A1/A	A2/A	A3/A	A4/A	A5/A	A1/B	A2/B	A3/B	A4/B	A1/C	A2/C	A3/C
Management (M)	Décision et organisation	M1	9.0	25.0													
	Elaboration stratégie	M2	9.0	25.0													
	Programmation	M3	25.0	25.0													
	Maîtrise de la Qualité	M4	25.0	25.0	12.0												
	Prospective	M5		20.0	12.0												
Réalisation (R)	R&T	R1				15.0					25.0				20.0		
	Avant projets	R2							20.0		20.0						
	Projets	R3					15.0								10.0		
	Opérations	R4					12.0				15.0						
	Collecte	R5					16.0				16.0						
	Préparation	R6					15.0										16.0
	QBD	R7					16.0							16.0			
	Approvisionnements	R8				20.0									10.0		
	Distribution	R9				22.5					22.5						
	Biothèque	R10						25.0									20.0
Soutien ou support (S)	Achats	S1			22.5					20.3				12.0			15.0
	Ventes	S2							15.0							16.0	
	Maîtrise de l'information	S3			16.0			20.0									
	Sécurité du travail	S4							16.0			25.0				16.0	
	Ressources humaines	S5			16.0			16.0						16.0		12.3	
	Ressources financières	S6		25.0													
	Sûreté et protection	S7			16.0					16.0							
	Communication externe	S8	20.0			20.0											
	Juridique	S9	25.0			20.0											
	Contrôle qualité	S10								15.0				16.0			
		Max	25.0	25.0	22.5	22.5	16.0	25.0	20.0	20.3	25.0		25.0	16.0	20.0	16.0	20.0
		Moy	18.8	24.2	15.8	19.5	14.8	20.3	17.0	17.1	19.7		25.0	15.0	13.3	14.8	17.3
		Min	9.0	20.0	12.0	15.0	12.0	16.0	15.0	15.0	15.0		25.0	12.0	10.0	12.3	16.0

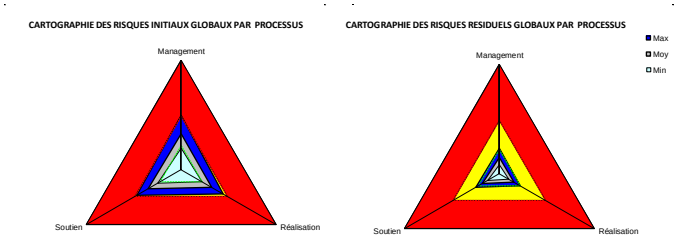

Fig. 13. Cartographies « Système » des risques initiaux et résiduels par processus (diagramme de Kiviat)

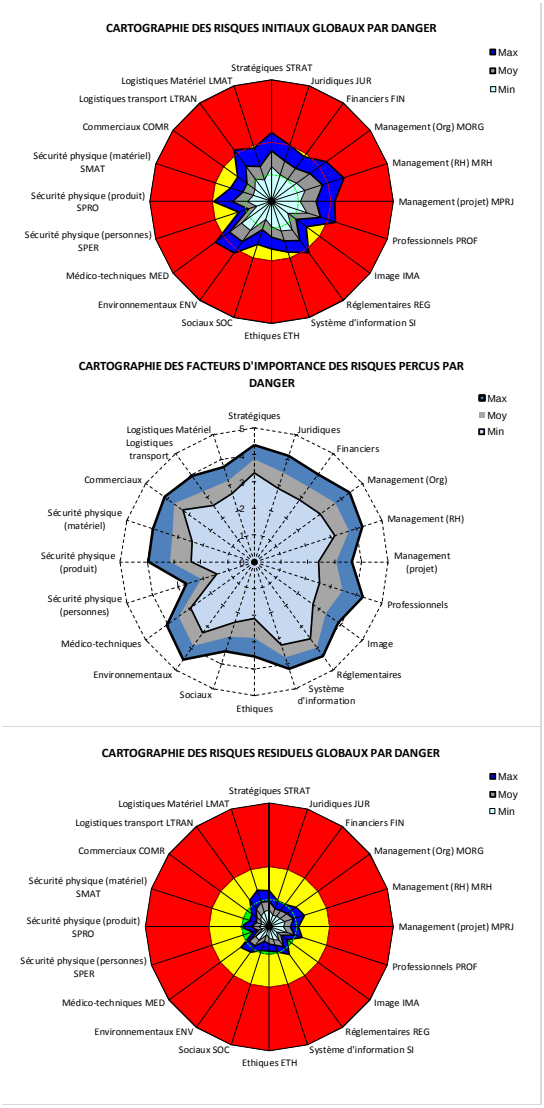

Fig. 14. Cartographies « Systèmes » des risques initiaux et résiduels (diagrammes de Kiviat), et cartographie des efforts perçus pour les sous-processus

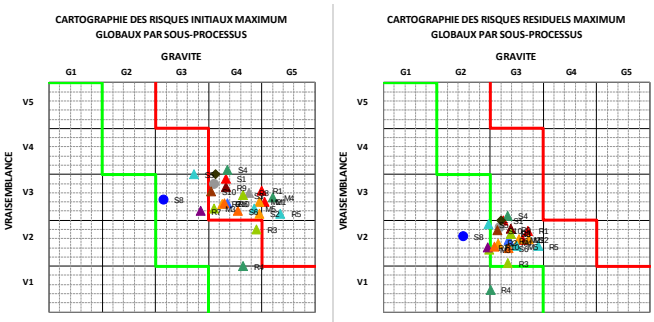

Fig. 15. Cartographies « Système » des risques maximums initiaux et résiduels (diagrammes de Farmer)

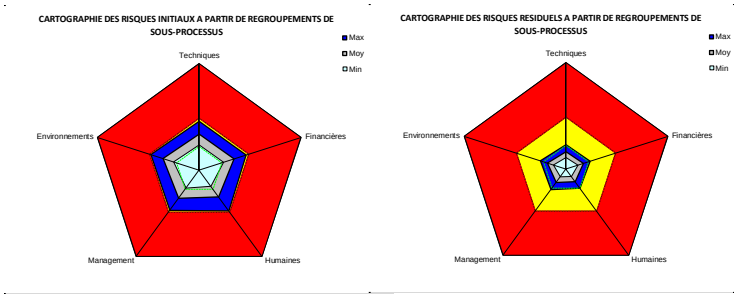

Fig. 16. Cartographies « Système » des risques initiaux et résiduels par cibles d'impact (regroupement des sous-processus)

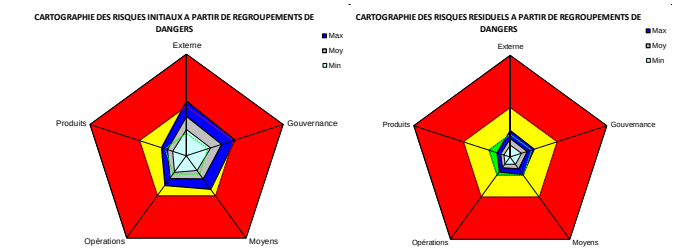

Fig. 17. Cartographies « Système » des risques initiaux et résiduels par catégories de dangers d'entreprise (regroupement des sous-processus)

L'ensemble des cartographies dont sont issus les exemples présentés ici fournit un diagnostic complet des risques à tous les niveaux de l'entreprise. Ils permettent d'identifier :

- les processus, sous-processus et activités critiques (dont les risques initiaux sont considérés comme inacceptables) ;
- les dangers génériques qui sont à l'origine des risques les plus critiques, à tous les niveaux ;
- les efforts perçus comme nécessaires pour réduire ces risques ;
- les risques résiduels résultant de la mise en œuvre de l'effort perçus.

Ces cartographies fournissent non seulement les niveaux de risques moyens, mais aussi les risques minimum et maximum. Ces intervalles min-max représentent à la fois la dispersion des valeurs des différentes activités pour un sous-processus ou processus donné, mais aussi la dispersion des valeurs recueillies des paramètres lorsqu'une même activité est auditée plusieurs fois (si par exemple elle est répartie sur plusieurs sites). L'analyse de cette dispersion est tout aussi fondamentale que celle des valeurs moyennes et peut mettre en évidence des dysfonctionnements ou des perceptions hétérogènes d'un même danger, hétérogénéité qui trahit souvent des problèmes de fonctionnement.

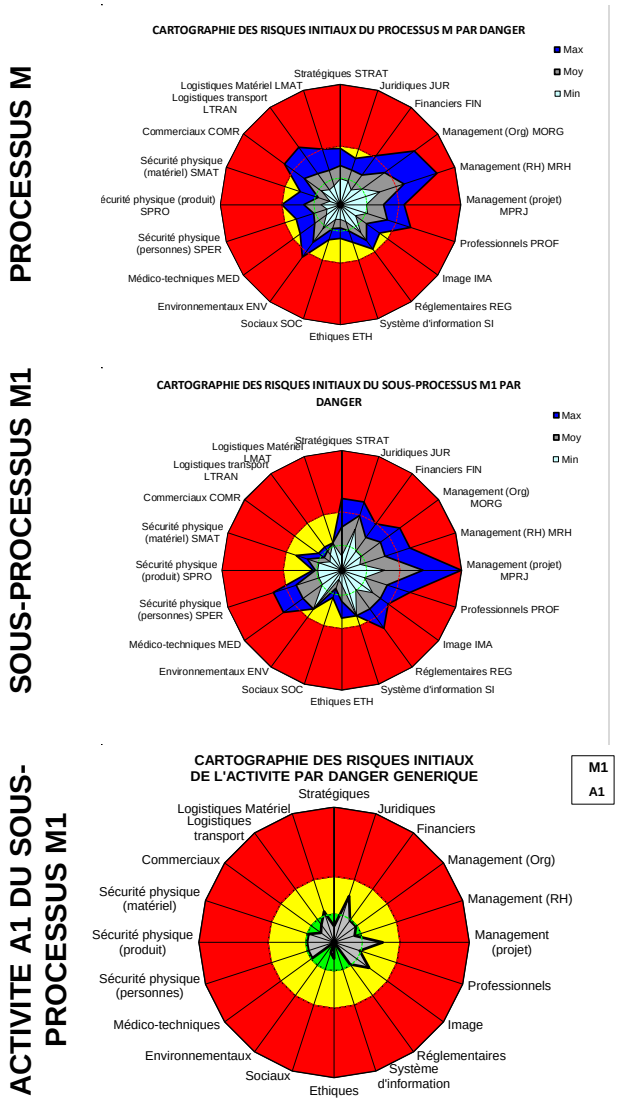

Fig. 18. Exemples de cartographies « Système » des risques initiaux et résiduels par dangers (diagramme de Kiviat)

V. Conclusion

La macro-cartographie des risques par audits est une méthode statique. La complexité du système analysé est implicitement prise en compte à travers la finesse de la description de ses processus, sous-processus et activités qui le modélisent. Celle-ci est visualisée par le plan d'audits. Le caractère dynamique est obtenu par l'évolution des environnements dangereux auxquels le système est exposé et par la récurrence périodique des audits.

A raison d'une à deux heures par audit, le recueil des données est très rapide et peu coûteux, surtout en s'appuyant sur les auditeurs internes déjà en place dans l'entreprise. De plus, les données d'audits internes ou externes déjà existantes peuvent utilisées pour établir le plan d'audit de la macro-cartographie ou pour renseigner les entrées de l'analyse. L'application de la méthode a été validée avec succès dans de grandes entreprises (CNES, EFS [8], SHAM [9]).

A l'issu de la macro-cartographie des risques par audit :

- un premier plan d'action de maîtrise des risques doit être mis en place afin de réduire les risques initiaux inacceptables ou tolérables sous contrôle, afin de les rendre acceptables ou de les maintenir à un niveau tolérable. La réalisation de ces actions doit être planifiée et programmée, et les résultats doivent être mesurés, en réalisant par exemple de nouveaux audits ciblés ;
- des analyses de risques plus fines, comme l'AGR [1] doivent être menées sur les activités et fonctions qui apparaissent les plus critiques. L'AGR permet de détailler les risques au niveau des sous-systèmes ou des fonctions, en identifiant les situations dangereuses, les facteurs de risques (causes contact, causes amorces), les événements redoutés ainsi que leurs conséquences et en évaluant les risques initiaux et résiduels associés. L'AGR aboutit au plan de maîtrise des risques (plan d'action de réduction des risques initiaux et catalogue des paramètres de sécurité pour la gestion des risques résiduels), accompagné d'une analyse du financement du risque (coûts des risques sans action et coûts des actions). Cette dernière est indispensable pour la prise de décision, qui peut être économique quand le coût de traitement est inférieur au coût du risque non traité, politique quand le coût du risque non traité est supérieur au coût du traitement.

References

[1] Desroches A, 2013. Le management des risques par l'analyse globale des risques, Transfusion Clinique et Biologique, Volume 20, Issue 2, pp 198-210, ISSN 1246-7820, http://dx.doi.org/10.1016/j.tracli.2013.02.002.

[2] Desroches A, et al., 2010. Le management des risques des entreprises et de gestion de projet. Ed Hermes science.

[3] Desroches A, et al., 2009. Principes et pratiques de l'analyse préliminaire des risques. Ed Hermes science.

[4] Cooper D. F. et al., 2005. Project Risk Management Guidelines – Managing Risk in Large Projects and Complex Procurements.

[5] Loosemore M., et al., 2006. Risk management in projects. 2nd Edition. Ed Taylor and Francis.

[6] Norme ISO 31000:2009. Management du Risques – Principes et Lignes Directrices.

[7] Norme ISO 9001:2008. Systèmes de management de la qualité.

[8] Sghaier W, 2014. Méthode systématique de reconception des processus intégrant la maîtrise des risques : contribution à la réingénierie des processus de l'EFS. Thèse de 3ième cycle. Ecole Centrale Paris.

[9] Monnot V., 2012. Cartographie des risques des établissements de santé sur la base d'audits : point de vue de l'assureur. Thèse professionnelle de l'Ecole Centrale Paris