

Enterprise-wide risk management

Contribution au développement d'outils permettant
la mise en place d'une gestion globale et intégrée dans les organismes

Jean-Paul A.Louisot

Docteur ès Sciences de Gestion

Paris I – Panthéon - Sorbonne (UFR 06 Gestion)

mars 2015

Edité par

B et K Management

33, rue Galilée – 75116 Paris

B et K Management
33 rue Galilée - 75116 Paris

ISSN : 1632-3106

Code ISBN : 978-2-916673-36-9

Le Code de la propriété intellectuelle et artistique n'autorisant, aux termes des alinéas 2 et 3 de l'article L.122-5, d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective ». Toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause, est illicite (alinéa 1er de l'article L. 122-4). Cette représentation ou reproduction, par quelque procédé, que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code pénal.

Ce livre reprend le support de la thèse soutenue le 17 décembre 2014. Il est dédié tout d'abord à mes parents qui nous ont quittés mais dont ce doctorat est en quelque sorte le couronnement de l'éducation qu'ils nous ont donné à ma sœur et à moi-même.

Mais je ne veux pas oublier tous ceux qui ont contribué à cette réflexion au premier rang desquels je dois citer Georges-Yves Kervern dont la vision scientifique et sociétale est à la source des cindyniques et surtout de l'hyper-espace du danger.

Parmi mes collègues avec qui j'ai travaillé à la formation du MP2 GGRC au sein de l'URF8 de l'Université Paris Panthéon Sorbonne pendant dix ans, je veux penser plus particulièrement à Viviane Balland qui m'a appris le temps long, au Professeur Pierre Pech qui m'a toujours encouragé, et a en outre présidé le jury de soutenance, et à Sophie Gaultier-Gaillard avec qui j'ai partagé et je partage encore recherches et articles.

Enfin je dois remercier le Professeur Jean-Paul Laurent d'avoir accepté de m'encadrer dans cette démarche inhabituelle, les deux rapporteurs, le Professeur Pierre Picard et le Professeur Gilles Motet et les autres membres du jury, le Professeur Michael Adams de Bath University et le Professeur Denis Kessler, PDG de la SCOR, qui ont bien voulu nous accompagner.

Jean-Paul Louisot, ARM, FIRM
Docteur ès Sciences de gestion
MBA Kellogg School of management, North Western University, 1972
Ingénieur Civil des Mines
Licencié ès Sciences Économiques

Table des matières

Contribution au développement d'outils permettant la mise en place d'une gestion globale et intégrée dans les organismes.....	1
Présentation des travaux	6
Introduction	6
Apport à la construction d'une science de la gestion des risques.....	7
1 Partie 1 – Évolution de la gestion des risques	11
1.1 Les trois ères ou les trois aires	12
1.1.1 Ère de l'artisan.....	13
1.1.2 Ère de l'ingénieur	13
1.1.3 Ère du stratège.....	13
1.2 L'ERM – Gouvernance, Risques et Conformités	13
1.2.1 La relation intrinsèque entre gouvernance et risques.....	17
1.2.2 Les éléments fondamentaux d'un cadre de gouvernance	17
• L'impact de la culture de l'organisme sur la gouvernance et la gestion des risques	18
• Émergence d'obligations légales et réglementaires concernant l'ERM.....	19
1.3 Description, complexité et chaos	20
2 Partie 2 – Les fondements théoriques & pratiques	22
2.1 Gestion des risques & Stratégie	23
2.2 Standards et cadres de référence.....	24
2.3 ISO 31000:2009.....	27
3 Partie 3 – Contributions à un corps de doctrine & une boîte à outils.....	30
3.1 Le processus de gestion des risques – respectant ISO 31000 :2009.....	31
3.2 Diagnostic des risques – l'espace des vulnérabilités.....	31
3.2.1 Ressources.....	32
3.2.2 Aléas ou événements	36
3.2.3 Impact ou Impacts.....	39
3.2.4 L'espace des vulnérabilités	40
3.2.5 Le Nœud Papillon	41
3.3 Diagnostic des risques – La méthode des centres de risques	43
3.4 Diagnostic des risques – Analyse & évaluation des risques	45
3.4.1 Objectifs de l'analyse ou quantification des risques	45
3.4.2 Quantification des risques – son apport pour la réduction des risques	45
3.4.1.2 Quantification des risques – son apport pour le financement des risques.....	48
3.4.2 Méthodes de quantification des risques.....	49
3.4.2.1 Méthodes probabilistes.....	50
3.4.2.2 Méthodes à base d'expert.....	51
3.4.2.3 Méthodes mixtes – Les Réseaux Bayésiens	51
3.6 Le traitement des risques – Le plan de redéploiement stratégique	53
3.7 La gestion des risques à la réputation	55
3.7.1 Suivi des risques à la réputation au travers des neufs pilotes.....	57
3.7.2 La gestion des risques à la réputation : un élément vital de tout ERM	57
4 Partie 4 – Les problématiques émergentes et pistes de recherche.....	61
4.1 Business intelligence systems / Business Analytics	62
4.2 Sécurité, sureté et intelligence économique	63
Périmètres de la sécurité d'entreprise	63
4.3 Sécurité des systèmes d'information.....	64
4.3.1 Les risques liés à l'utilisation des SI.....	65
4.3.2 Risques liés aux ressources humaines	66
4.4 Gestion des risques de la chaîne logistique	66

4.5 Extension de l'approche de la logique floue à d'autres domaines que la gestion des risques à la réputation.....	69
4.5.1 Indice de résilience des collectivités territoriales	70
4.5.2 Indice de maturité de l'ERM	70
4.5.3 Indice de notation pour la finance islamique.....	70
Bibliographie.....	70
Bibliographie personnelle	74
Ouvrages.....	75
Articles.....	75
Articles académiques	76
Articles professionnels.....	76
Articles de vulgarisation	77
ANNEXE – Illustration par des cas de terrain	82
ANNEXE 1.....	84
ANNEXE 2.....	98

Présentation des travaux

Introduction

Ce que j'expose dans les pages qui suivent est un commentaire des livres et articles publiés au cours des vingt dernières années et qui représente un cheminement dans la gestion des risques.

Spectateur impliqué dans le quotidien comme courtier, assureur et risk manager j'ai appliqué une réflexion systématique à ce que devenait la gestion des risques sous mes yeux, depuis l'achat rationnel de couvertures d'assurance jusqu'à la gestion stratégique des risques qui se dessine actuellement.

Plutôt qu'une méthode scientifique traditionnelle, basée sur la réflexion théorique ou sur l'analyse de données empiriques, la plus fréquemment rencontrée dans les départements «risques & assurances» des universités américaines, et également asiatique, je me suis documenté en assistant aux principales conférences professionnelles du monde entier, Amérique du Nord, Europe et Australasie sans oublier l'Afrique au travers de l'enseignement et des conférences des assureurs.

Par ailleurs l'enseignement de la qualification professionnelle d'ARM à des générations de praticiens depuis 1994 a permis de confronter les idées avec des praticiens qui ont apporté leur contribution au murissement des outils.

C'est ce regard croisé, affiné par la rencontre avec Georges Yves Kervern et les Cindyniques, qui m'a permis de visualiser et d'anticiper le cheminement de la gestion des risques et de voir les points d'achoppement pour les praticiens. C'est donc à un effort de «*conceptualisation de l'expérience*» que je me suis systématiquement livré. C'est ainsi que j'ai pu déterminer les domaines de manque auquel je me suis efforcé modestement d'apporter des solutions :

- **Au niveau du diagnostic** L'espace des vulnérabilités et la méthode des centres de risques permettent effectivement de dialoguer avec les «*propriétaires de risque*» dans leur langage et avec des problématiques de performance qui les touchent directement. Il permet en outre de déboucher naturellement sur le plan de continuité nécessaire au niveau des opérationnels.
- **Au niveau du traitement** Le recours abusif au mot «*crise*» dans certaines entreprises et la nécessité de réagir au juste niveau aux situations de perturbation que peut vivre tout organisme. C'est ainsi qu'est né le plan de redéploiement stratégique.
- **Au niveau des risques spécifiques** La réalisation de l'importance croissante de la réputation, surtout avec l'avènement des médias sociaux, et la rencontre avec Jenny Rayner, et des spécialistes du suivi des médias ont contribué à la définition d'un modèle de gestion des risques à la réputation.

Achetez cet ouvrage,
exclusivement disponible sur RiskAssur-boutique

<http://riskassur-boutique.com/etudes-version-ebook-pdf/736-9782916673369.html>

Consultez, encore quelques pages, ci-après

Apport à la construction d'une science de la gestion des risques

La démarche que j'ai entreprise depuis 1973 vise à la conjonction de la réflexion théorique dont les apports sont essentiels, et l'expérience pratique sans laquelle aucune discipline de gestion ne peut exister. C'est ce que j'ai appelé la conceptualisation de l'expérience pour permettre aux leçons apprises dans une situation donnée d'être transposables à d'autres situations différentes dans le temps, l'espace et l'activité.

De fait, la gestion des risques a subi une évolution considérable au cours des six décennies depuis son émergence comme une fonction technique dans certaines entreprises américaines dont le budget assurances justifiaient de disposer d'un spécialiste interne pour encadrer les courtiers. Cette évolution résulte en partie du fait de la frustration des praticiens qui ressentaient les limites de l'exercice, en partie de la réflexion des universitaires d'horizons différents qui ont essayé de développer un support scientifique pour concevoir des instruments spécifiques.

C'est ainsi que les Cindyniques dont le nom apparut pour la première fois dans les pages du Monde le 10 décembre 1987, constituent une science dont la dernière définition posée est : « *Science visant à rendre intelligibles, et donc prévisibles, les dangers, les risques qui en découlent, endogènes et exogènes au sein d'un système et de permettre de les réduire.* »¹

Mais l'accélération du mouvement depuis vingt ans et plus particulièrement depuis la première décennie du XXI^e siècle est liée à la complexité croissante des interrelations entre les acteurs économiques, les interdépendances qui dépassent trop souvent la capacité de l'homme à les appréhender sans recours à la théorie de la complexité².

Dans un document récemment mis à jour, les auteurs du livre rouge OCEG³ notent que : « *L'environnement dans lequel les organismes évoluent est aujourd'hui plus complexe et plus exigeant que jamais. Même les PME/PMI, les organismes à but non lucratif, et les acteurs publics ont à relever des défis auxquels seules les grandes entreprises internationales étaient confrontées dans le passé. Les parties prenantes, internes et externes, ne se contentent plus de hautes performances, elles exigent en outre la transparence de la gestion. Les risques et exigences réglementaires qui pèsent aujourd'hui sur les organismes constituent un maquis dense et changeant qui peut frapper sans prévenir. Pour couronner le tout, les coûts à engager pour contrôler ces risques tendent à être hors de contrôle. En résumé, dans beaucoup d'organismes le statut n'est ni soutenable, ni acceptable.* »

L'explosion tant du périmètre d'exercice de la gestion des risques, que de son impact sur la vie de tous les responsables stratégiques et opérationnels suppose la mise au point d'une batterie d'instruments que tous comprennent et savent utiliser au quotidien. C'est dans ce contexte que les apports spécifiques auxquels j'ai contribué jouent un rôle dans l'ouverture des yeux des responsables pour qu'ils aient vraiment une vision 360° pour prendre leurs

¹ Kervern Georges-Yves, Philippe Boulenger , Cindyniques – Concepts et Mode d'emploi , Paris (France) : Economica, 2007 p.1

² Kervern Georges-Yves, Philippe Boulenger , Cindyniques – Concepts et Mode d'emploi , Paris (France) : Economica, 2007 p.1

³ OCEG, red book – GRC capability Model, Version 2.1, New-York (USA), 2012

3.1 Le processus de gestion des risques – respectant ISO 31000 :2009

Le processus de gestion des risques développé au cours de trente années de pratiques est globalement compatible avec ce que propose l'ISO 31000 :2009. La figure 3.1 reprend ce processus mis à jour pour assurer la complète harmonie avec la norme ISO 31000 :2009.

On retrouve effectivement :

L'établissement du contexte interne et externe qui dans le cadre de l'élaboration de la stratégie aboutit à la définition d'objectifs « *soutenables* » et la définition d'un appétit de risque ou tolérance au risque de l'organisme.

Le diagnostic de vulnérabilités (appréciation du risque dans l'ISO 31000) décomposé en trois sous-étapes : identification (quelles sont les aléas qui pèsent sur quelles ressources), analyse (quantification du risque brut) et évaluation (quantification du risque résiduel)

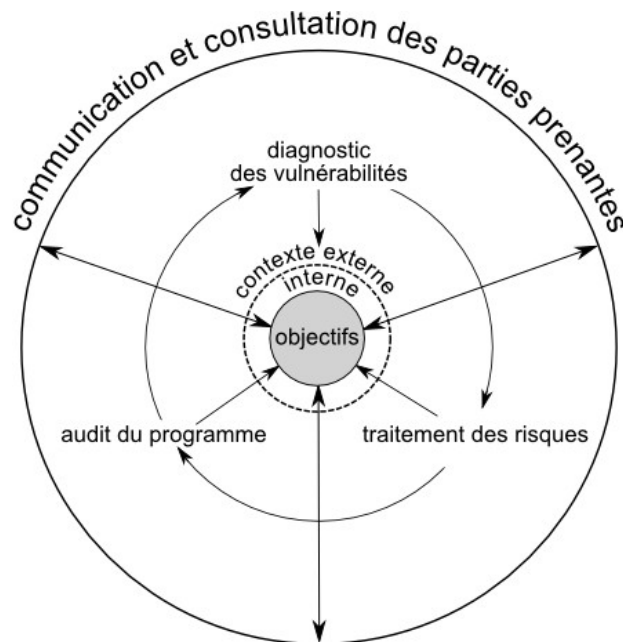


Figure 3.1: Processus de gestion des risques ARM, compatible ISO 31000

Le traitement des risques qui comprend la réduction et le financement

L'audit du programme de gestion des risque (pilotage et revu dans l'ISO 31000) qui vise à la fois la boucle de retour (amélioration continue) et les différents niveaux d'audit

Communication et consultation avec l'ensemble des parties prenantes.

3.2 Diagnostic des risques – l'espace des vulnérabilités

Une définition courante du risque qui dérive de la finance « *déviaton par rapport à l'espérance mathématique* »²⁹ mais cela n'est pas très opérationnel et ne permet pas un

²⁹ Segal Sim, Corporate value of Enterprise Risk Management, John Wiley & Sons, Hoboken, New Jersey (USA), 2011 p. 23

suivi avec des indices de performances. Certains auteurs hésitent encore sur les définitions, comme Cendrowski et Mair³⁰ qui définissent le risque comme la probabilité que survienne un dommage et la vulnérabilité comme le produit de la probabilité par l'impact ce qui pose la problématique de l'identification, par quels paramètres ?

L'approche que nous proposons ici pour la gestion des risques s'appuie sur un modèle qui décrit tout organisme comme un portefeuille de vulnérabilités, menaces et d'opportunités, chacune étant identifiée par trois paramètres :

- Une ressource ou objet de risques ;
- Un événement aléatoire, aléa ou péril (si on ne s'intéresse qu'au volet négatif) ;
- Un impact qui doit s'envisager comme les conséquences sur l'atteinte des objectifs de l'organisme mais sans oublier les aspects non financiers et la confiance des parties prenantes.

Nous allons passer en revue ces trois paramètres pour se doter d'un outil d'analyse de la situation de chaque organisme dans la perspective d'assurer son avenir en dépit des incertitudes qui pèsent sur lui.

3.2.1 Ressources

Tout organisme peut être défini comme une combinaison dynamique de ressources, pour atteindre des objectifs. La définition de ces objectifs est donc au cœur de la gestion de tout organisme.

Il va, toujours, s'agir de combiner les ressources de la façon la plus efficace pour atteindre l'objectif le plus ambitieux possible avec les ressources déterminées, ou d'atteindre l'objectif désigné avec le moins de ressources possibles. Il s'agit de la définition, même, de l'efficacité pour l'affectation des ressources dans une économie libérale.

Il existe de nombreux modèles découpant les entreprises ou les organismes en un nombre variable de ressources. Pour l'utilisation pratique en gestion des risques, nous retiendrons cinq catégories qui permettent une approche globale de l'organisme, en distinguant des classes, dont les modes de traitement des risques qui sont associés sont spécifiques à chacune d'elle comme nous le verrons plus loin.

H = Humaines il s'agit, ici, de l'ensemble des personnes liées à l'organisme par des contrats de travail ou des mandats, et dont les compétences, formations et expériences spécifiques, en font un véritable actif pour l'entreprise. Il faudrait prendre en compte, également, les données démographiques telles que : âge, sexe, situations de famille, qui peuvent avoir un impact sur la capacité de produire. En un mot, ce sont les éléments pris en compte, parce qu'il est traditionnel d'appeler : gestion des compétences ou « *knowledge management* » ou mieux encore aujourd'hui la gestion des talents.

³⁰ Cendrowski Harry, Mair William G., Enterprise Risk Management & COSO, John Wiley & Sons, Hoboken, New Jersey (USA), 2009

**Achetez cet ouvrage,
exclusivement disponible sur RiskAssur-boutique**

<http://riskassur-boutique.com/etudes-version-ebook-pdf/736-9782916673369.html>

Consultez, encore quelques pages, ci-après

Enterprise-wide risk management

Contribution au développement d'outils permettant la mise en place
d'une gestion globale et intégrée dans les organismes

Jean-Paul Louisot

mars 2015

Edité par

B et K Management

33, rue Galilée – 75116 Paris

Code ISBN

978-2-916673-36-9

