

Sommaire

Avant-propos	XV
1 Introduction	1
1.1 La gestion de l'incertitude par un processus stratégique continu..	3
1.2 La prise de décision en avenir incertain	11
2 La gestion des risques stratégiques ou la gestion stratégique des risques ?	15
2.1 La perception du risque et l'appétit de risques	15
2.2 La genèse de la gestion des risques	22
2.3 L'éthique, le développement soutenable et la gouvernance (ESG)	23
3 Les fondements de la gestion des risques	27
3.1 La stratégie de gestion des risques : fixer des objectifs à la gestion des risques	27
3.2 Les processus de gestion des risques	28
3.3 Le rôle et l'importance des <i>business intelligence</i>	31
3.4 La spécificité des territoires : de la gestion des risques à la bonne gouvernance	33
4 L'ERM : une approche efficiente pour gérer les incertitudes .	37
4.1 L'amélioration de la prise de décision	38
4.2 L'amélioration de la communication sur les risques	44

5	L'amélioration des procédures de la gestion stratégique grâce à l'ERM	55
5.1	L'amélioration de la prise de décision stratégique.....	56
5.2	L'intégration de l'ERM dans le processus d'élaboration de la stratégie.....	57
5.3	La définition des objectifs de l'ERM (établir le contexte interne et externe).....	58
5.4	L'analyse et l'évaluation des risques et l'établissement des priorités pour les risques critiques (diagnostic des risques ou appréciation des risques).....	60
5.5	Le traitement des risques critiques et la prise en compte des priorités (traitement des risques).....	62
5.6	Le suivi des risques critiques (audit – surveillance et revue).....	62
5.7	L'émergence d'obligations légales et réglementaires concernant l'ERM.....	64
6	La comparaison entre la gestion des risques traditionnelle et l'Enterprise-wide Risk Management	67
6.1	Les catégories de risques prises en compte	68
6.2	L'intégration dans le processus de développement de la stratégie	69
6.3	Les métriques utilisées pour évaluer la performance atteinte	72
6.4	Le cadre organisationnel.....	73
6.5	La gestion des risques et la gestion du changement.....	77
7	Le management des risques et de la résilience	81
7.1	Les objectifs de la gestion des risques et la résilience	81
7.2	L'évolution et l'explosion du <i>risk management</i> et la conduite du changement.....	83
7.3	Les différentes visions de la résilience : le cœur du débat	85
8	Les problématiques émergentes	89
8.1	La crise économique et la gestion des risques.....	89
8.2	La gestion des risques a-t-elle un problème structurel ?.....	90
8.3	Des trois lignes de défense aux cinq lignes d'assurance raisonnable.....	93
8.4	L'insertion de l'analyse quantitative des risques dans tous les aspects de l'organisme	97

8.5	L'optimisation de la performance des organismes en avenir incertain.....	104
8.6	L'univers de la sécurité et du risque dans la tourmente réglementaire	105
8.7	Une petite histoire de la gestion des risques	106
8.8	Un univers des risques en pleine évolution et la nécessité d'anticiper.....	107
8.9	L'approche gouvernance/conformités et gestion des risques (GRC).....	108
8.10	L'apport de la norme ISO 31000:2009 et ses implications.....	109
8.11	La stratégie et la gestion des risques	110
8.12	L'intelligence économique comme moteur du rapprochement sécurité et risques.....	111
8.13	Un marché pour répondre aux attentes des acteurs.....	113
8.14	La gestion de la sécurité, la gestion des risques et la création de valeur.....	114
8.15	De l'approche GRC à l'approche SRC : stratégie, gestion des risques et changement	114
8.16	Conclusion et perspectives	115
	Annexes	119
	Annexe 1 Les principaux cadres de référence et standards de la gestion des risques.....	121
	COSO 2	122
	FERMA (pour mémoire).....	123
	AS/NZS 4360 (pour mémoire remplacé par AS/NZ 31000) .	124
	BS 31100.....	126
	ISO 31000:2009.....	126
	ONR 49000:2014.....	127
	Bâle 2 et 3 – Solvabilité 2	128
	Sous-cadres de référence spécialisés	130
	Annexe 2 Comment renforcer la résistance aux risques ? Les dix « meilleures pratiques »	133
	Rapport d'étape sur la problématique de la gestion de la résilience.....	137

Annexe 3	Le rapport Walker sur la gouvernance d'entreprise	141
Annexe 4	Gouvernance, risque, conformité, nouveau <i>mantra</i> de la gestion des risques : triangle d'or ou triangle des Bermudes ?	147
	La relation intrinsèque entre gouvernance et risques.....	150
	Les éléments d'un cadre de référence typique pour la gouvernance	151
	L'impact de la culture d'entreprise sur la gouvernance et la gestion des risques	152
Annexe 5	Les enjeux et la stratégie de formation à la gestion des risques dans le cadre d'un projet ERM.....	155
	L'état de l'art	157
	La problématique	165
	La création d'un service de gestion des risques <i>corporate</i> ..	168
	Conclusion	171
	Bibliographie	172
Annexe 6	La huitième directive européenne sur la gouvernance : les trois lignes de défense ?	175
	L'organisation de la défense.....	176
	La recherche d'un langage commun	177
	Commentaires personnels de l'auteur	178
Annexe 7	L'ISO 31004 : la mise en œuvre de la norme ISO 31000:2009, une longue marche sans fin	181
	L'ISO 31004 pour la mise en œuvre de l'ISO 31000:2009 ...	182
	Des nouvelles perspectives pour la gestion de la sécurité ouvertes par l'ISO 31000 ?	182
	La perspective canadienne sur la mise en œuvre de la norme ISO 31000:2009.....	186
	Et la route continue... ..	189
Annexe 8	L'entreprise responsable ou la responsabilité d'entreprise ?	191
	Pourquoi une stratégie de soutenabilité ?	195
	Qu'est-ce que le dialogue actif avec les parties prenantes ou parties intéressées ?.....	196

Comment obtenir l'adhésion des collaborateurs ?.....	197
L'investisseur responsable est-il en train de monter en puissance ?.....	198
Et pour conclure... provisoirement en attendant une nouvelle version de l'ISO 31000	200
Annexe 9 Le <i>management</i> des risques et de la résilience	203
Les objectifs de la gestion des risques et la résilience.....	203
L'évolution et l'explosion du <i>risk management</i> et la conduite du changement.....	205
Les différentes visions de la résilience : le cœur du débat...	207
Bibliographie	211
Annexe 10 La rupture stratégique ou la stratégie de rupture ?	213
La rupture stratégique.....	214
La rupture stratégique : le débat à l'École militaire.....	216
Les stratégies de rupture : une définition.....	220
Les stratégies de rupture et l'innovation	221
Les stratégies de rupture et les règles du jeu.....	223
La rupture stratégique et les ressources humaines.....	223
La rupture stratégique et l'information	224
La rupture stratégique et la veille.....	226
La rupture stratégique : maturité et création de sens	227
La rupture stratégique : innovation et <i>management</i> des risques	228
La rupture stratégique et la stratégie de rupture.....	231
Annexe 11 Les auditeurs internes : piliers de contrôle et agents de changement	233
Pourquoi l'autorité de contrôle de la comptabilité est-elle partie prenante ?.....	234
La cyber sécurité relève-t-elle du comité d'audit ?	236
L'approche intégrée GRC est-elle le cheval de Troie des auditeurs dans le domaine des risques ?	238
Quels sont les dix risques clés en 2015 ?	240
Quel rôle partagé pour l'audit et le <i>risk management</i> dans le changement ?.....	242

Comment organiser la coopération entre <i>risk management</i> et audit interne ?	246
Annexe 12 Les lanceurs d’alerte :	
vigies citoyennes ou traîtres ?.....	249
Le contexte extra-juridique	251
Le lanceur d’alerte est-il un déviant au sens de la sociologie ?	257
Le contexte juridique mondial	259
Les ateliers spécialisés sur le contexte juridique français ...	264
Le rapport d’étape en guise de conclusion	266
Bibliographie	268
Annexe 13 Vingt ans après... l’ARM	271
Comment a été entreprise la longue marche de l’ARM en francophonie ?	272
Pourrait-on oublier le rôle des cindyniques ?	273
Pourquoi fallait-il créer l’EFARM ?	274
Créer l’ <i>Enterprise-wide Risk Management Practitioner</i> (ERMP), une ardente obligation ?	276
Où en est la greffe de l’ARM sur AMRAE Formation ?	278
Quelles sont les perspectives pour les vingt prochaines années ?	281
Bibliographie	282
Annexe 14 La gestion des risques stratégiques ou la gestion stratégique des risques ?	285
Petite histoire et perspectives de la gestion des risques	285
Les trois ères ou les trois aires ?	287
L’ERM : gouvernance, risques et conformité	291
L’impact de la culture de l’organisme sur la gouvernance et la gestion des risques	296
La gestion des risques à la réputation	297
Une citation en guise de conclusion	300
Annexe 15 L’attention du <i>risk management</i> change de cible	301
Annexe 16 « L’entreprise citoyenne »	303

Annexe 17 Pourquoi faut-il un indice de maturité de l'ERM ?	305
Le contexte actuel de la gestion des risques.....	305
Le modèle ébauché et la piste de recherche.....	306
Et la route continue	310
Glossaire.....	310
Annexe 18 Les Bermudes hissent la voile	313
Quel est l'impact des indiscrétions du Panama sur les Bermudes ?	314
Quels efforts ont permis d'obtenir l'équivalence Solvabilité 2 ?.....	316
Les Bermudes s'intéressent-elles à l'Afrique ?.....	318
Quels sont les avantages des Bermudes comme domiciliation d'un assureur ?	318
Pourquoi le congrès Alarys aux Bermudes ?	320
Les Bermudes envisagent-elles de diversifier leur économie ?	321
Alors où vont les Bermudes après l'équivalence Solvabilité 2 ?.....	322
Annexe 19 Le RIMS invite ses membres à repousser leurs limites	325
Où va le terrorisme ?	326
Cyber risques, doit-on redouter les attaques sur les infrastructures critiques ?	327
Cyber risques, où en est l'assurance ?.....	329
Qu'en est-il de l'ERM en Amérique latine ?	331
L'ERM, mode passagère ou nécessité vitale pour les organismes ?	333
Comment prendre des risques avec efficacité ?	335
ERM et continuité doivent-elles se rapprocher ?.....	336
Comment faciliter une réunion « Risques » de façon efficace ?	338
Comment faire face de mieux en mieux à la complexité ?	340

Avant-propos

L'analyse des fondements théoriques qui sous-tendent la plupart des approches de la gestion enseignées au sein des MBA de toutes les Grandes Écoles de gestion, comme dans les cycles de formation des hauts fonctionnaires, laisse l'universitaire confondu tellement elles semblent en être restées à l'atome de Démocrite, et, si on est généreux, l'atome de Bohr. Autrement dit, ces enseignements restent fondés pour la plupart sur la conception classique de la physique et de l'information, celle qui a conduit certains États à concevoir des plans rigides à cinq ans... Les États ont abandonné cette pratique avec la chute de l'Union Soviétique, alors même que de nombreuses entreprises sont encore gérées comme si le monde évoluait à un pas de sénateur... Mais tel n'est pas le cas ! En clair, les acteurs économiques et les dirigeants politiques qui n'ont pas tiré les conséquences de l'abandon du plan en restent pour l'essentiel à une lecture déterministe de l'avenir.

Le fondement de la physique traditionnelle est le suivant : à mêmes causes, mêmes effets, ou à causes proportionnelles, effets proportionnels. Il a été remis en question de façon fondamentale par les évolutions modernes de la microphysique, ces avancées sont résumées dans le principe d'incertitude, ou des relations d'incertitude exprimées par Heisenberg. Cette recherche qui a, d'une certaine manière, ouvert la voie de la théorie du chaos ne semble pas encore avoir influencé de façon systématique la réflexion stratégique, même si certains dirigeants visionnaires s'en inspirent, peut-être même sans le savoir. On pense, bien entendu, à ceux qui ont forgé notre présent et continuent de forger le futur comme le fondateur d'Apple® ou celui de Google®. Mais sans

doute sont-ils nombreux, animateurs anonymes dans les ETI et les PME/PMI, elles qui sont au cœur de la création d'emplois et de richesses dans les pays développés, comme dans les pays émergents ?

En clair, sans trop caricaturer, les processus stratégiques utilisés aujourd'hui dans les organismes sont trop rigides et séquentiels car ils se fondent sur l'idée d'un monde dont l'évolution est contrôlable et progressive. En réalisant, seulement périodiquement, des analyses de leur contexte interne et externe, ces organismes se privent d'une vision en continu dans laquelle les signaux faibles permettraient d'anticiper efficacement les évolutions et les révolutions futures pour garantir le maintien de la pertinence de l'organisme au sein de son réseau d'acteurs.

Bien entendu, les grands acteurs économiques, comme les États, ont les moyens de s'appuyer sur des modèles de plus en plus puissants et même qui apprennent : « Nos systèmes apprennent par eux-mêmes de l'expérience, mais c'est nous qui décidons de ce sur quoi ils apprennent. Toutefois, le jeu même complexe est plus accessible aux ordinateurs que des problèmes généraux du monde réel. »¹

Les tenants de l'intelligence artificielle restent eux-mêmes prudents sur le remplacement de l'humain par la machine dans les décisions complexes. Werner Heisenberg lui-même a remis en cause l'utilisation de loi normale des probabilités pour lire son principe, ouvrant ainsi la voie aux extrêmes... aux ruptures.

En ce qui concerne la physique quantique, W. Heisenberg a indiqué que, puisque la position exacte et le moment d'une particule ne peuvent pas être connus à un instant donné, le futur ne peut pas être déterminé. On ne peut pas calculer sa trajectoire précise mais seulement un éventail de trajectoires possibles (en utilisant l'équation d'Erwin Schrödinger, on peut calculer avec précision les probabilités de différentes trajectoires). Le problème est que je ne crois pas que le monde économique ait pu définir l'équivalent de l'équation de Schrödinger pour un monde dont les variables sont très complexes et, sans doute, avec des interactions que même la logique floue aura du mal à modéliser. Comment osons-nous prétendre prévoir avec précision l'avenir alors que nous ne comprenons pas même les détails du présent ?

Pour le monde du risque et pour les professionnels de la gestion du risque, la bonne nouvelle est que l'incertitude et le risque sont au cœur de toutes les décisions, tant au niveau stratégique et tactique qu'opérationnel, donc tout

.....
1 Denis Hassais, fondateur de DeepMind.

le monde appartiendrait aux *risk managers*. La mauvaise nouvelle est que de nombreux professionnels d'horizons divers ont compris l'importance du chantier, depuis les auditeurs internes et externes avec les trois lignes de défense, en passant par les qualitatifs, l'ISO 9000:2015 comprend un volet risques, sans oublier les spécialistes de la sécurité, de la sûreté, de l'intelligence économique, pour n'en nommer que quelques-uns. La concurrence est donc rude !

Pour que l'avenir de la fonction de *risk manager*, fut-il ou elle appelé(e) CRO, encore si jeune, une ou deux décennies tout au plus, soit assuré dans un tel maelstrom, encore faut-il que les praticiens se hissent à la hauteur des enjeux.

La gestion des risques est une fonction de dirigeants : ils doivent déterminer et conduire la politique de leur organisme en prenant en compte les incertitudes. Mais, sans relais à tous les niveaux, elle n'aurait aucune chance de succès. C'est aussi une mission pour tous les acteurs, publics et privés. C'est de la vigilance de chacun, que dépend la survie de tous... Cela doit rappeler des souvenirs précis à ceux issus du monde des sections spéciales de la gendarmerie ou de la police !

De plus, l'irruption généralisée des médias sociaux, qui s'invitent désormais dans tous les grands débats, implique une transparence qui peut être en conflit avec la rapidité de décision qui s'impose lorsque les prémices d'une rupture exigent une révision déchirante de stratégie. Et cependant, rien ne sera possible si le changement n'est pas embrassé par tous, au sein de l'organisme comme à l'extérieur, dans son réseau de partenaires. C'est pour cela que le processus continu de réflexion stratégique doit être éclairé par une gestion des risques intégrée et globale et positionnée dans une gestion du changement au sein de laquelle tous ont le sentiment d'être écoutés et entendus.

Dans un tel contexte, la question de la démocratie dans l'entreprise, qui avait tant agité les jeunes soixante-huitards dont j'étais, se pose de façon très différente. Il n'y a sans doute pas de modèle unique de chemin vers la démocratie. Tantôt elle surgit de la base, tantôt elle est imprimée par le sommet, mais le succès passe par une conjonction des deux. Les dirigeants doivent vouloir le changement, mais encore faut-il que l'ensemble des personnes intéressées l'adopte. Il n'y a pas de stratégie unique qui mette en place les instruments de la résilience et c'est bien le cas de la gestion des risques et des concepts et méthodes proposées par l'ISO 31000.

Toutefois, dans un monde devenu trop complexe et imprévisible pour se prêter à des approches déterministes ou à la vision d'un seul homme, l'*Enterprise-wide Risk management* (ERM) propose une démarche qui place l'incertitude au cœur de toute décision dans un organisme. De plus, par son approche *top-bottom* et *bottom-up*, elle assure l'adhésion de tous au processus de changement permanent, alors même que le changement est ce qui inquiète le plus les hommes et les femmes au sein de la société, comme au sein de l'entreprise. Sans doute s'agirait-il également, sans sortir du capitalisme, de ramener les pays occidentaux au niveau d'inégalité d'avant les années quatre-vingt².

Je décevrai sûrement ceux qui cherchent des recettes. Cet ouvrage n'est pas un livre de cuisine mais un questionnement sur tous les défis que doit relever tout entrepreneur, tout cadre dirigeant, à tout homme politique face aux incertitudes de demain et d'après-demain pour faire avancer la société, même en temps de chaos. L'ERM vise à optimiser la prise de risques : saisir les opportunités tout en contenant les menaces. Il est donc au cœur de toute stratégie d'entreprise.

Si le risque du changement climatique n'est que peu mentionné, c'est qu'il existe de nombreux ouvrages qui en parlent en détail, ainsi que les mesures de prévention et de protection que l'on pourrait imaginer. Bien entendu, aujourd'hui, aucun organisme ne pourrait se tracer une trajectoire à horizon 2025/2040 sans le prendre en compte dans ses réflexions stratégiques, il est source de bien des menaces, mais également d'opportunités pour les innovateurs !

Professeur Jean-Paul Louisot,

Docteur ès Sciences de Gestion de la Sorbonne
MBA, ARM, FIRM

.....
2 Atkinson Anthony B. *Inéga*liés. Traduit de l'anglais par Françoise et Paul Chemla avec une préface de Thomas Piketty, Paris, Éditions du Seuil, 2016.