

Etude de la généalogie et des enjeux de la norme de gestion des risques ISO 31000

Pierre FORT, Marco PEREIRA, Virginie ZAYOUN – sous la direction de Soraya BOUDIA

Master 2 Ingénierie des risques, Université Paris Descartes

Plan de l'article

Contexte	1
Retour sur le contenu de la norme	2
Généalogie de la norme	3
De la technique à la gestion, une évolution conceptuelle majeure.....	4
Un standard non certifiable pourquoi ?	6
Atouts et limites de l'outil générique	7
Pistes d'évolution de la norme	7
Conclusion.....	9
Bibliographie	10

MOTS-CLÉS : RISQUE – MANAGEMENT - NORME – ISO 31000 – ENJEUX - GENEALOGIE

Contexte

Cet article est issu de la création d'un groupe de travail portant sur un instrument de gestion des risques, la norme iso 31000, composé de trois étudiants de l'Université Paris Descartes en Master 2 Ingénierie des Risques, a pour objectif de mieux comprendre la généalogie et les enjeux de cette nouvelle norme de gestion des risques. Afin de répondre à nos interrogations, nous avons réalisé dans un premier temps un état de l'art des documents portant sur la norme. Nous avons pu constater qu'il existait peu de travaux la concernant et que son contenu restait méconnue d'un certains nombres de gestionnaires des risques. Nous nous sommes intéressés dans un second temps aux membres de la commission chargés de la rédaction de la norme. Nous avons décidé de consulter un maximum de ces acteurs afin de disposer de plusieurs opinions venant de profils variés tels que des chercheurs travaillant dans des agences de santé publique ou des risk-managers issus de grandes entreprises Françaises. Parmi toutes les personnes contactées nous avons pu obtenir un accord pour trois interviews. Ces interviews ont pris la forme d'entretiens téléphoniques. Le premier avec M. Gilles Motet, Professeur à l'Institut National des Sciences Appliqués de Toulouse (INSAT) et ancien Directeur Scientifique de la Fondation pour une Culture de Sécurité Industrielle (FonCSI). Gilles Motet a participé aux travaux du groupe « Evaluation des risques » de l'Afnor et a représenté la France dans le groupe de travail « Risk Management » de l'ISO en charge de la rédaction de la norme ISO 31000 « Risk Management – Principles and guidelines ». De

plus il a publié au sein de la FonCSI et des « cahiers de la sécurité industrielle » un document s'intitulant « La norme iso 31000 : 10 questions¹ » à travers lequel il explique les enjeux de cette norme. Ce texte a notamment servi de base à nos travaux de recherches. La deuxième personne interviewée est M. Bruno Debray, chercheur à l'Institut National de l'Environnement Industriel et des Risques (INERIS) et responsable d'une unité spécialisée dans l'évaluation des risques industriels. Bruno Debray a été mandaté par l'INERIS pour participer à la commission de normalisation ISO 31000 après avoir participé à un programme de formalisation des connaissances dans le domaine des risques majeurs. Notre troisième contact est M. Yves Merian, membre de l'Institut pour la Maîtrise des Risques (IMdR) où il occupe la fonction de président de la commission « Réglementation et Normalisation ». Yves Merian a été amené à travailler sur les risques et la norme ISO 31000 par le biais du domaine de la continuité d'activité et de la gestion de crise. Il était notamment responsable d'un pôle « continuité d'activité » au Ministère de l'Economie et s'est beaucoup intéressé aux plans de continuité d'activité dans le secteur privé.

Nous tenons à fortement remercier ces trois experts Français pour leurs participations et leurs commentaires qui nous ont été plus que précieux dans la rédaction de cet article. Nous remercions également M. Jean Pierre Petit, délégué général à l'IMdR, de nous avoir guidé et aidé dans nos recherches.

¹ Gilles Motet, 2009, *La norme iso 31000 : 10 questions*, Les cahiers de la sécurité, FonCSI, Toulouse, 21 pages.

Retour sur le contenu de la norme

Avant de discuter de la généalogie et des enjeux de la norme, revenons un instant sur son contenu. La norme ISO 31000 : Management du risque – Principes et lignes directrices a été publiée en novembre 2009 par l'Organisation Internationale de Normalisation. Elle est décrite comme fournissant les « principes génériques et les lignes directrices pour la mise en œuvre efficace du management du risque dans les organismes² ». Elle se décompose en cinq grandes parties qui sont :

1. Le domaine d'application : cette partie décrit les cibles de la norme. Elle est présentée comme pouvant être « appliquée par tout public, toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu ». La norme peut s'appliquer à n'importe quelle étape de la vie d'une organisation et peut s'appliquer à tout type de risque et « que ses conséquences soient positives ou négatives ».
2. Les termes et définitions : ce chapitre permet de définir tous les termes importants de la norme. Il prend une place très importante car il apporte une nouvelle définition du mot risque « effet de l'incertitude sur l'atteinte des objectifs ». Dans notre entretien Bruno Debray qualifie cette nouvelle définition de « révolutionnaire » et explique qu'elle peut être déroutante pour des personnes habituées à qualifier le risque comme un danger

associé à une probabilité. Il souligne cependant son intérêt à rendre plus explicite la notion d'acceptabilité et le caractère intentionnel de la maîtrise des risques.

3. Les principes : dans cette partie sont décrits onze principes que les organismes doivent respecter pour avoir un « management des risques efficace » :
 - Le management du risque crée de la valeur et la préserve ;
 - Le management du risque est intégré aux processus organisationnels ;
 - Le management du risque est intégré au processus de prise de décision ;
 - Le management du risque traite explicitement de l'incertitude ;
 - Le management du risque est systématique, structuré et utilisé en temps utile ;
 - Le management du risque s'appuie sur la meilleure information disponible ;
 - Le management du risque est adapté ;
 - Le management du risque intègre les facteurs humains et culturels ;
 - Le management du risque est transparent et participatif ;
 - Le management du risque est dynamique, itératif et réactif au changement ;
 - Le management du risque facilite l'amélioration continue de l'organisme.

4. Le cadre organisationnel : ce chapitre décrit le cadre organisationnel de management des risques pour que les

² Afnor, 2007, *Evolution de la norme iso 31000*, Concepts – Principes et Réalité, 28 pages.

ETUDE DE LA GENEALOGIE ET DES ENJEUX DE LA NORME DE GESTION DES RISQUES ISO 31000

principes ci-dessus soient respectés et que le processus de management des risques présenté ci-dessous fonctionne. Cette partie détaille l'importance d'établir une politique de management des risques et introduit les notions d'engagement et de responsabilité des organisations.

5. Le processus : cette partie apporte des conseils pour intégrer un « processus de management des risques » dans une organisation. Ce processus est découpé en cinq activités :
- La communication et concertation ;
 - L'établissement du contexte ;
 - L'appréciation du risque ;
 - Le traitement du risque ;
 - La surveillance et revue.

Nous avons pu constater à travers son contenu que la norme ISO 31000 cherche à harmoniser la manière de gérer le risque en apportant un cadre général. Mais quelle est l'origine de cette norme et comment est-elle venue s'insérer dans un univers d'ores et déjà très normalisé ?

Généalogie de la norme

L'ISO 31000 est une norme internationale sur le management du risque publiée en 2009 par l'Organisation internationale de normalisation. L'ISO est une organisation internationale non gouvernementale, indépendante, composée de 162 organismes nationaux de normalisation. Une norme ISO se construit selon six stades, le stade de proposition qui consiste à confirmer qu'il existe un besoin, le stade de préparation où un groupe de travail est mis en place pour préparer le projet, le stade de comité où est rédigé la norme au format ISO, le stade de

l'enquête où le projet de norme est soumis aux divers comités, le stade d'approbation où le projet final de la norme internationale est soumis au vote et enfin le stade de publication où le texte est publié par le secrétariat central de l'ISO en tant que norme internationale. L'AFNOR s'est chargée de retranscrire la norme internationale en norme Française au travers de sa commission de normalisation, présidée par Pierre PEYROUTY. Cette commission de normalisation est composée d'acteurs venant de milieu public ou privé très variés, IRSN, INERIS, AFNOR, SNCF, TOTAL, MEDEF, DIRECTION GENERALE DU TRAVAIL etc...

Dès 2004 en France l'INERIS en collaboration avec l'AFNOR a travaillé sur la question de la gestion des risques ce qui a donné la norme FD X50252 Management du risque - Lignes directrices pour l'estimation des risques. Cette norme est distribuée sous forme de fascicule à destination des entreprises et des institutions Française afin d'amorcer un processus d'harmonisation du langage et des pratiques dans divers secteurs traitant de divers risques. Bruno DEBRAY : « *L'objectif de ce fascicule de documentation à usage uniquement français à l'époque, était déjà d'apporter un cadre un peu global d'évaluation des risques en essayant de faire quelque chose qui puisse être mis en œuvre aussi bien pour des gens qui traitent de risques industriels que par des gens qui traitent de risques naturels par exemple. [...] C'était une première tentative au niveau français d'unifier un peu les concepts dans le domaine, où finalement on se rendait compte conceptuellement que tout le monde avait une approche à peu près similaire mais en terme de vocabulaire, en terme de description de cette approche, il pouvait y avoir des différences assez importantes. L'idée était de faire converger un peu les choses. »*

La norme ISO 31000 fournit des principes génériques et des lignes directrices pour la mise en œuvre efficace du management du risque dans les organismes. Elle est applicable à n'importe quel organisme, indépendamment de sa taille et de son secteur d'activité. Elle cherche également à harmoniser le processus de management du risque et les définitions qui sont rattachées dans les normes existantes et futures. Gilles MOTET : *« L'objectif de la norme c'était d'être une norme chapeau c'est-à-dire une norme qui devait être multi sectoriel, multi risque, [...] sinon il y aurait eu un désaccord, et il n'y aurait pas eu de consensus entre les différents experts. »*

Avant l'ISO 31000 il existait déjà de nombreuses normes sur les aspects de gestion des risques, spécifique à des technologies, secteur ou domaine d'activité. La question de l'intérêt de la norme dans ce contexte se pose donc naturellement, mais en réalité l'objectif principal était de passer outre les spécificités de chacun pour poser de manière ferme mais discutée un langage et une approche commune sans obligatoirement apporter des choses nouvelles. Gilles MOTET sur la question, *« L'intérêt de l'ISO 31000 n'est pas obligatoirement d'apporter quelque chose de nouveau, enfin il y a des choses nouvelles à mon avis dedans, mais c'était surtout d'arriver à fournir aux gens un cadre commun, des vocabulaires communs, une approche commune, de façon à permettre par exemple à des gens qui sont sur des risques financiers de dialoguer avec des gens qui sont dans domaine de la sécurité, de plus en plus il y a des problèmes de couplage, on ne peut pas séparer les risques comme cela. Il faut avoir une vision commune, une approche commune. »*

Au niveau international, une proposition du comité Japonais appuyée par les comités Australien et Britannique sur un nouveau sujet d'étude pour l'élaboration de lignes directrices pour le management des risques a été approuvée en juin 2005. Cette proposition s'inscrit dans un contexte où, mondialement l'intérêt et le besoin d'une telle norme se faisaient sentir. Sans cette vague les travaux n'auraient pas eu lieu. Ainsi ces travaux sur l'ISO 31000 présidés par l'Australien Kevin W KNIGHT ont officiellement commencé en septembre 2005. L'Australie était déjà en avance en matière de management des risques notamment grâce à sa norme AS/NZS 4360, c'est cette norme qui a servi de base aux travaux sur l'ISO 31000.

De la technique à la gestion, une évolution conceptuelle majeure

Nous l'avons vu dans les chapitres précédents, la norme se veut universelle et applicable à tous systèmes de management des risques. On observe par ailleurs, au travers de la norme une évolution conceptuelle du risque qui de notre opinion traduit bien la volonté de standardisation du langage en matière de management des risques.

En effet, nos interviews ont toutes trois révélé cette problématique bien connue dans le management des risques : « on parle la même langue mais pas le même langage » ; jusqu'ici les définitions du risque étaient ainsi associées aux notions de danger et/ou de probabilité³. La

³ Gilles Motet, « Le concept de risque et son évolution », Annales des Mines -

définition du risque donnée dans la norme est la suivante : « *effet de l'incertitude sur l'atteinte des objectifs* »⁴. Intéressons-nous à cette dernière.

Cette nouvelle définition, intègre les effets potentiels positifs de l'incertitude, le risque n'est donc plus obligatoirement associé à un danger et/ou à une probabilité d'occurrence. Cette évolution sémantique, offre ainsi une signification plus large au mot risque, et répond de ce fait à ce besoin de standardisation. En effet, le mot comprend donc les significations que l'on peut lui attribuer aussi bien dans le domaine environnemental, que financier, industriel ou la santé au travail tout en prenant en compte les aspects positifs liés à l'incertitude. « *Au point de départ c'est une norme qui a été conçue avec l'idée d'unifier les démarches d'évaluation des risques financiers, évaluation des risques globaux pour l'entreprise et pour les indemnisations, et autres démarches d'évaluation des risques. Elle a une forte teinte risques financiers ou risques globaux.* » nous a fait remarquer Mr Debray. C'est effectivement principalement dans le domaine financier que le risque est bien souvent associé à de l'opportunité. Quand on achète des actions en bourse, il s'agit d'une opportunité qui se révèle être un risque par exemple.

Gilles Motet, l'un de nos interviewés, s'est intéressé à l'évolution du concept de risque ainsi qu'à la norme ISO 31000 au travers de deux articles respectivement dédiés à chacune de ces thématiques (confère bibliographie). Il

Responsabilité et environnement 2010/1 (N°57), p. 32-37.

⁴ ISO/IEC 31010:2009 PDF version (EN/FR)

estime et nous le rejoignons, que les lois probabilistes utilisées généralement pour estimer la probabilité d'occurrence d'un évènement partent d'un postulat : celui que « *le passé est le prolongement du futur* ». Cette nouvelle définition « non probabiliste » semble donc être plus proche de la réalité.

Cette nouvelle façon d'aborder le risque illustre également à notre sens, l'esprit de la norme. Celle-ci, comme nous l'avons précédemment évoqué, sort de la technique et de la statistique. L'ingénieur étudiait le danger, le statisticien la probabilité d'occurrence du risque. Le management des risques était de ce fait plutôt confié aux techniciens. La tendance aujourd'hui est de confier ce management à des spécialistes gestionnaires. La norme se situe donc à un niveau plutôt stratégique, relativement loin des aspects opérationnels et donc techniques. Au-delà de l'évolution conceptuelle que nous avons évoquée cela traduit également un réel changement de paradigme dans la gestion des risques. L'efficacité dans la maîtrise des risques se situerait plutôt dans le cadre organisationnel donné pour la gestion des risques et non plus dans l'expertise technique ?

« *L'oppositif objectif de la norme c'était d'être une norme chapeau c'est-à-dire une norme qui devait être multi sectorielle, multi risque, et donc si jamais on déclinait la norme avec un niveau trop bas on se rapprochait des moyens, et là les moyens à ce moment-là sont vraiment dépendent des secteurs d'activités, des technologies, donc cela semblait extrêmement difficile d'arriver à un accord au niveau international. Au tour de la table il y avait aussi bien des gens qui avaient des préoccupations différentes, par exemple : le risque financier, tout ce qui s'oriente au safety, prévention des accidents majeurs, risque*

projet... Donc si nous voulions vraiment faire une norme multisectorielle, multi domaine, il fallait se placer à un certain niveau d'abstraction, sinon il y aurait eu un désaccord, et il n'y aurait pas eu de consensus entre les différents experts. » Gille Motet

Un standard non certifiable pourquoi ?

La norme ISO 31000 n'ouvre pas à la certification. Nous nous sommes intéressés aux raisons de cette décision de l'ISO. Pourquoi au contraire d'autres normes comme l'ISO 9001, relative au management de la qualité ou l'ISO 14001 qui s'intéresse aux questions environnementales le sont ? L'ISO 31000 prend-elle la forme d'un guide plutôt que d'une norme à suivre stricto-sensu ? Un guide par ailleurs, pour lequel les organismes souscripteurs ne peuvent ainsi prétendre à un certificat à utiliser comme gage de « qualité » dans la gestion des risques. Nous avons donc posé la question successivement à nos trois interviewés. Ces derniers nous ont respectivement apporté les réponses suivantes :

Gilles Motet : « Il y a des raisons plutôt politiques, il y a eu l'opposition de deux pays dont la France et l'Allemagne essentiellement. Alors pourquoi ces deux pays-là ? Ce n'est pas toujours très clair, il y a eu surtout une opposition venant des ministères. Est-ce que ça vient du fait que les ministères avaient peur qu'il y est une exigence, une demande de certification des populations par exemple, le principal gestionnaire du risque c'est le gouvernement et l'administration, soit liée à la santé, via la police etc... Ce sont des gens qui gèrent des risques. Donc est-ce qu'il n'y aurait pas eu derrière une demande ? Il y a des

domaines de l'administration dans certains pays qui sont mis en conformité avec l'ISO 31000, je pense par exemple au Canada, il a une partie de l'administration Canadienne qui a adopté le cadre de l'ISO 31000. Après est ce que c'est vraiment fondamental d'avoir un élément de certification, je ne sais pas, je ne suis pas très convaincu. Il y avait un intérêt financier derrière la certification. C'est une énorme manne financière et donc il y avait des pressions importantes de certaines sociétés plutôt que des pays, pour amener à la certification, les gens se rendaient compte que derrière il y avait du boulot et de l'argent à se faire. »

Yves Merian : « Ce n'est pas une norme certifiable parce que précisément c'est difficile de mesurer et d'évaluer de façon précise ce qui se passe quand on manage des risques. »

M. Debray : « C'est plus un document structurant qu'un document prescripteur. Le fait qu'elle ne soit pas certifiante c'est aussi un choix ... Le monde industriel s'est globalement opposé à ce qu'elle soit certifiante. Alors pourquoi ? C'est parce que finalement une norme certifiante, oblige une mise en application très rapide car on observe un phénomène d'uniformisation qui poussent ceux qui ne sont pas certifiés à le faire. En effet, ceux qui ne sont pas certifiés se retrouvent peuvent se retrouver coincés car des clients vont demander à ce qu'ils le soient.

Je pense qu'elle ne contient pas non plus d'éléments qui soient suffisamment précis en termes de prescriptions pour que l'on puisse facilement certifier la conformité d'un système à cette norme.

Par contre, je pense qu'elle fournit un très bon cadre. Si vous avez une organisation et que vous vous demandez comment vous pouvez appréhender le management des risques, qu'est-ce que vous devez faire ? Et bien la norme vous fournit tous les ingrédients de ce à quoi vous devez réfléchir, à la fois en termes d'organisation et en termes de processus. »

Si l'on se réfère à nos trois interviewés les raisons pour lesquelles la norme n'est pas certifiable sont diverses mais relèveraient essentiellement d'une opposition de la part des politiques et des industriels. Par ailleurs il semblerait difficile d'évaluer au travers d'un audit la conformité d'un système de management des risques à la norme ISO 31000.

Atouts et limites de l'outil générique

La norme est donc un outil générique de gestion des risques applicable à tout système de management des risques, peu importe le domaine d'activité concerné. Mais quels sont les atouts ainsi que les limites de cet outil ? Nous avons interrogé nos trois experts à ce sujet :

Gilles Motet considère que l'un des atouts essentiels est le côté multisectoriel de la norme. Bruno Debray, pense quant à lui que la norme fournit un cadre global intéressant mais qui peut se révéler être lourd à appliquer. L'avantage serait l'aspect « cadre global » qui peut nécessiter cependant une petite gymnastique intellectuelle. « Si on se place au niveau d'une entreprise ou d'une organisation ou pourra s'appuyer sur cette norme pour

mettre en place, pour définir un certain nombre de choses.

Moi ce caractère là je le trouve très intéressant et je trouve aussi intéressant le fait qu'elle soit très riche. Le côté négatif est un peu le pendant de cela. Elle reste aussi assez conceptuelle et générale, dans certains domaines. L'appliquer directement peut être très lourd, du coup elle propose un cadre qui est très général, qui peut sembler assez lourd. Finalement quand on fait de la gestion des risques à une échelle très locale et sur des problématiques très spécifiques, la norme c'est un énorme pavé par rapport à une action concrète qu'on doit mettre en œuvre. »

Yves Merian, rejoint Bruno Debray mais considère comme un atout le fait qu'un langage commun est pu être déployé au travers de la norme : « Le premier avantage est qu'elle soit sortie. Il faut arriver à trouver un langage commun au niveau international... et cela est compliqué. Elle sert donc de « repère ». Elle a aussi l'avantage d'avoir donné une définition du risque dans un monde où chaque métier va le définir d'une manière différente. La nouvelle définition a pour vocation de faire partager une notion commune entre les différents métiers afin que tout le monde s'y retrouve. Ça c'est un gros progrès parce que les gens ont tendance à nous dire « il n'y a pas de risque parce que je ne peux pas le mesurer. »

Pistes d'évolutions de la norme

La publication de la révision de la norme ISO 31000 est prévue pour mai 2018. Les normes ISO font l'objet d'une révision tous les cinq ans. Cette révision s'inscrit donc dans une suite logique. Nous allons donc essayer de vous donner quelques pistes d'évolutions qui nous

ont été soumises lors de nos recherches. Cela nous permettra également de discuter des perspectives.

Tout d'abord il semblerait que certains acteurs dont la France ne souhaitent pas que la structure de la norme évolue fondamentalement afin de laisser le temps aux organismes et entreprises de digérer la norme telle qu'elle est actuellement, étant donné que l'ISO 31000 est récente dans le paysage normatif. De plus les processus de management normatif prennent généralement deux à trois ans pour être déployés et encore plus pour devenir mature.

Yves Merian : *La révision va être plutôt technique. Comme la norme est encore relativement récente, il n'est pas question aujourd'hui, en tout cas du point de vue Français, de faire une révision qui transformerait l'architecture de cette norme. Les révisions viseront à améliorer la lisibilité pour prendre en compte des choses qui ont été introduites dans d'autres normes et ainsi, faciliter les croisements.* »

Le grand chantier évoqué par Yves Merian et Gilles Motet est, l'intégration du management des risques à l'intérieur d'autres systèmes de management. Nous définirons ceci de « *management intégré* ». Cette volonté de management intégré est une vision à plus long terme de l'ISO. L'ISO 9001 sur le management de la qualité en est la preuve, car elle ouvre grand les portes à l'évolution de l'ISO 31000 en intégrant lors de sa révision en septembre 2015 un chapitre sur les risques et les opportunités. Cette évolution normative ne se limite pas à des couples de normes. C'est-à-dire que l'ISO 9001 n'ouvre pas seulement des portes à l'évolution de l'ISO 31000 mais aussi à celles d'autres normes telles que l'ISO 22301 sur la continuité des activités. De plus ce

mouvement de management intégré est suivi par une vague de simplification normative. Nous reprendrons l'exemple récent et couronné de succès de la simplification de l'ISO 9001. En toute logique, l'ISO 31000 devrait suivre ce mouvement. De plus une des critiques récurrente des normes ISO porte sur le nombre de normes. En réalité cette critique est plus complexe, elle peut dépendre de la culture et de la perception d'un pays, d'une organisation, mais aussi de sa taille. En effet il est plus simple pour une grande entreprise que pour une PME d'attribuer des moyens à la mise en place de systèmes de management issus des normes ISO.

Yves Merian : « *La culture germanique s'oppose à la création d'un trop grand nombre de normes de système de management [...] la culture anglophone approuve au contraire ce système.* »

Concernant le management intégré :

Gilles Motet : « *Au niveau des systèmes de management actuels, vous avez des approches un peu différentes en fonction des domaines. [...] de plus en plus, les systèmes de management sont intégrés. On va tenter de coupler les choses. Pour cela il nous faut avoir un cadre commun, la nouvelle version de l'ISO 31000 intégrera cette approche. Enfin il ne faut pas voir le management du risque comme quelque chose d'isolé mais comme un élément particulier du mangement.* »

Yves Merian : « *Il persiste des interrogations quant à l'articulation de cette norme (ISO 31000) avec d'autres systèmes de management qui sont aussi couverts par des normes [...] un questionnaire a été créé pour discuter de ce point, il est nécessaire que son utilisation puisse se faire de manière « homogène ».* »

Un grand débat s'est ouvert autour de la prise de décisions et de l'articulation autour du

décisionnaire. Faut-il, éviter le risque, prendre le risque, éliminer la source du risque, modifier la probabilité d'apparition ou les conséquences, partager ou maintenir le risque... ? La norme doit-elle être prévue comme un outil d'aide à la réflexion ou un outil de décisions. Les experts ne s'accordent pas sur le sujet. Cela ouvre également le sujet sur l'implication de la direction dans ce processus complexe qu'est la prise de décisions. Quelle légitimité ? Comment prendre une décision sur un risque que je ne subis pas ? Cette révision sera sous doute encore fortement animée autour de ces approches.

Une autre piste d'évolution est l'amélioration de la communication. En effet, ce n'est pas un sujet aussi simple qu'il y paraît, et qui peut vite devenir sensible. Par exemple, comment doit-on communiquer ses risques avec ses différentes parties prenantes ? Cela nécessite de communiquer sur ses menaces et ses vulnérabilités. Or dans le contexte actuel, crise, terrorisme... Il devient très compliqué pour les organismes et les entreprises de communiquer là-dessus. Quelles sont les informations que l'on peut donner ou pas, et à qui ? Un début de réponse peut se trouver aujourd'hui dans la dernière version de l'ISO 9001. Il est donc fort probable que la révision de l'ISO 31000 traite plus ou moins en profondeur de ce sujet.

INERIS, quant à elle propose comme piste d'évolution pour la norme, un guide d'application spécifique pour chaque secteur et domaine d'activité, ceci pouvant permettre d'aider les PME qui ne sont pas forcément bien armées pour se lancer dans l'ISO 31000. De plus cela pourrait réconcilier avec la norme les personnes qui trouvent qu'analyser les risques est une perte de temps.

Bruno Debray : « *Je pense qu'il faudrait des guides d'application qui essayent de décliner la norme iso dans différents secteurs et qui apportent une harmonisation et un enrichissement des pratiques et des méthodes de management* »

Conclusion

L'ISO 31000 est une norme internationale sur le management du risque publiée en 2009 par l'Organisation internationale de normalisation. Cette norme non certifiante a pour origine la norme Australienne AS/NZS 4360. Elle est « révolutionnaire » dans sa manière d'aborder les risques puisqu'elle essaye d'harmoniser la gestion en apportant un cadre général. Elle peut être qualifiée de norme « chapeau » et se fixe pour objectif de permettre à des gens issus de secteurs variés de disposer d'un vocabulaire et des processus communs. La norme innove en apportant une nouvelle définition du risque présenté comme « l'effet de l'incertitude sur l'atteinte des objectifs ». Le risque n'est donc plus uniquement lié à un danger et une probabilité, il inclut également la potentialité « bénéfique » du risque. Cette définition permet de correspondre à une population plus large dont les gestionnaires des risques financiers. Le caractère « non certifiant » de la norme s'explique par des divergences politiques au niveau mondial et des réticences du monde organisationnel et industriel qui ne souhaite pas se retrouver coincé face à des clients qui exigeraient la certification. La révision prévue pour mai 2018 ne devrait pas changer fondamentalement la structure de la norme, mais poursuivre l'orientation de l'ISO qui consiste en un mouvement de simplification de ses normes, ainsi que à leurs intégrations dans divers systèmes de management. (Qualité,

environnement, sécurité...) Néanmoins de nombreuses interrogations restent en suspens sur l'orientation de la communication vers les parties intéressées et le champ décisionnel.

Bibliographie

Articles :

- Gilles Motet, 2010/1, *Le concept de risque et son évolution*, Annales des Mines - Responsabilité et environnement (N°57), p. 32-37.
- Gilles Motet, 2009, *La norme iso 31000 : 10 questions*, Les cahiers de la sécurité, FonCSI, Toulouse, 21 pages.
- Afnor, 2007, *Evolution de la norme iso 31000*, Concepts – Principes et Réalité, 28 pages.

Normes :

- ISO 31000:2009 *Management des risques*. Organisation Internationale de Normalisation
- ISO 9001:2015 *Management de la qualité* Organisation Internationale de Normalisation

Sites internet :

- AFNOR, Commission de Normalisation Management des risques
http://www2.afnor.org/espace_normalisation/structure.aspx?commid=55774 (Consulté le 25/01/16)
- Institut pour la maîtrise des risques, *Conférences sur l'ISO 31000*
<http://www.imdr.eu/Menu/ACTIVITES/Manifestations+IMdR/Manifestations+IMdR+Passees/p-137.html>
(Consulté le 25/01/16)