Pre-print en diffusion libre autorisée
Publication consultable ici : https://doi.org/10.1016/j.irbmnw.2017.02.001

Adoptez l'ISO 31000 pour un management du risque performant

O. Aby-Salami[1], D. El Haouli[1], F. Konté[1], O. Mansour[1], I. Motte[2], B. E. Ouali[1*], G. Farges[1*,]

[1] Master Qualité et Performance dans les Organisations
[2] Mastère Spécialisé Normalisation, Qualité, Certification, Essai
Université de Technologie de Compiègne, CS 60319, 60203 COMPIEGNE CEDEX FRANCE
*site web : www.utc.fr/master-qualite - *correspondants : o.bahae@gmail.com / gilbert.farges@utc.fr*

Les enjeux du management du risque

Le risque a toujours accompagné l'homme depuis son existence. Ce dernier l'a intégré dans son mode de fonctionnement pour assurer sa survie.

Au fil du temps, le développement des sociétés, l'ouverture des marchés et les avancées technologiques ont donné naissance à de nouveaux types de risques, allant des simples risques industriels aux risques stratégiques. Les organismes évoluent dans un environnement de plus en plus incertain, fluctuant et interdépendant, mettant en cause la pérennité de leurs activités.

La succession d'évènements tragiques au cours du XXème siècle ont mis en évidence l'importance de la gestion des risques avec entre autre des risques : industriels (explosion du site industriel Total « AZF » [1]), financiers (la crise des subprimes [2]), sociétaux (les soulèvements du monde arabe [3]) et humains (l'épidémie du virus « Ebola » [4]). C'est ainsi qu'est apparu, dans les années 1960, le terme « Risk management » [5] ou management des risques, qui peut être appliqué à tous les processus d'un organisme. Afin d'uniformiser les pratiques de gestion de risque à travers le monde et de les rendre compatibles à tout type d'activité, l'ISO 31000 « Management du risque – Principes et lignes directrices » a été publiée en 2009 [6] avec une révision programmée pour 2017. Elle fournit des recommandations afin de faciliter l'intégration du management du risque.

Les organismes, quelques soient leurs types, leurs secteurs et leurs tailles (entreprise, gouvernement, Organisation Non Gouvernementale (ONG), individu, etc.) sont confrontés à une multitude de risques qui constituent des incertitudes à l'atteinte de leurs objectifs. En 2016, les organismes ont deux objectifs primordiaux : d'un côté, développer l'innovation dans la quête d'offrir le produit le plus attractif et/ou conquérir de nouveaux marchés. Et d'un autre côté, garantir un haut niveau de sécurité en maîtrisant les risques souvent engendrés par ces processus.

Afin de les gérer de manière efficace, chaque organisme doit identifier et classer ses risques en fonction de ses enjeux prioritaires. D'une manière exhaustive, Jean-David DARSA a déterminé 11 catégories de risques présentées dans la figure 1, touchant tous les secteurs associés à la vie de tout type d'organisation [7], [8].

Catégorie de risques	Exemples
Risques géopolitiques	Blocus économique, attentat, guerre, climat insurrectionnel, …
Risques économiques	Inflation, évolution de la demande, du besoin, du marché, …
Risques stratégiques	Incohérence entre les différents segments constitutifs du modèle stratégique
Risques financiers	Illiquidité, taux de change, risque de crédit, dilution du capital, …
Risques opérationnels	Engendrés par l'infrastructure, l'énergie, le cycle de production, …
Risques industriels	Liés à l'activité de fabrication, de transformation, …
Risques juridiques	Contrefaçon, responsabilité pénale du dirigeant, …
Risques informatiques	Liés aux matériels, logiciels, applications, infrastructures réseaux, …
Risques sociaux ou psychosociaux	Perte d'homme-clé, mal-être, stress, harcèlement sexuel, suicide, …
Risques d'image ou de réputation	Contrefaçon, rumeur, concurrence déloyale, espionnage industriel, …
Risques de knowledge management	Perte de connaissance et de savoir-faire

Figure 1 : Les catégories de risques d'après Jean-David DARSA [7], [8]

Selon une étude réalisée en 2012 par la fédération des associations de management du risque en Europe, FERMA (Federation of European Risk Management Associations), le nombre de participants à ce type de sondage, réalisé tous les deux ans, a augmenté de 49 à 809 participants entre 2002 et 2012 [9]. Cette augmentation montre bien que de plus en plus d'organismes sont intéressés par le management du risque. Cette même étude a aussi porté sur les référentiels utilisés et il s'est avéré que l'ISO 31000 devient un référentiel de choix pour intégrer le risque management.

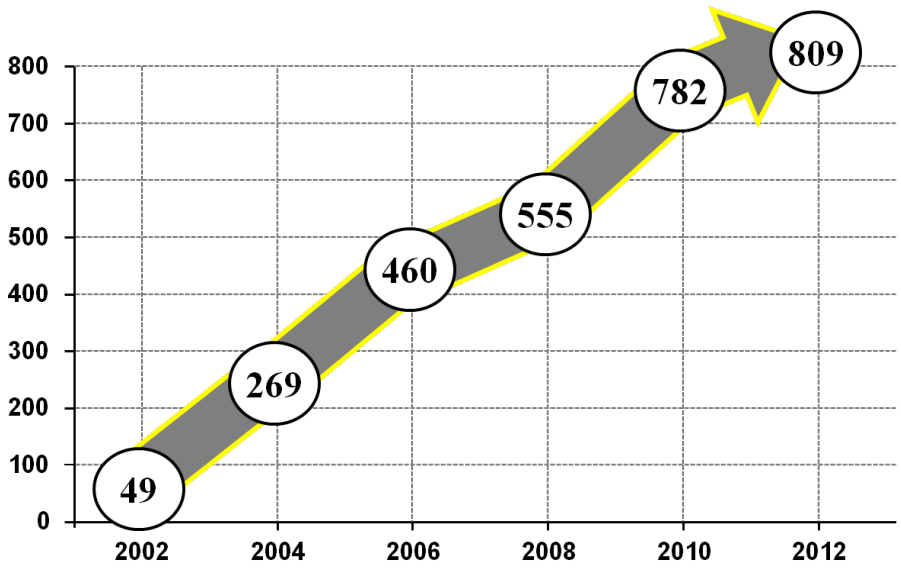

Figure 2 : Évolution du nombre d'entreprises intéressées par le management du risque en Europe selon FERMA [9]

Trois normes internationales appartenant à la famille de l'ISO 31000, traitent du management du risque. L'ISO 31000 énonce les principes et les lignes directrices pour toute forme de risque rencontrée dans les organisations. L'ISO 31004 « Lignes directrices pour l'implémentation de l'ISO 31000 » [10] et l'ISO 31010 « Gestion des risques – Techniques d'évaluation des risques » [11] en sont, quant à elles, des supports. Le lien entre ces trois normes peut se résumer dans la figure 3. Elles constituent une solution

efficace pour aider les organismes à déployer leur approche risque de façon structurée et vont amener de la performance en anticipant les effets des risques à tous les niveaux de l'organisme.

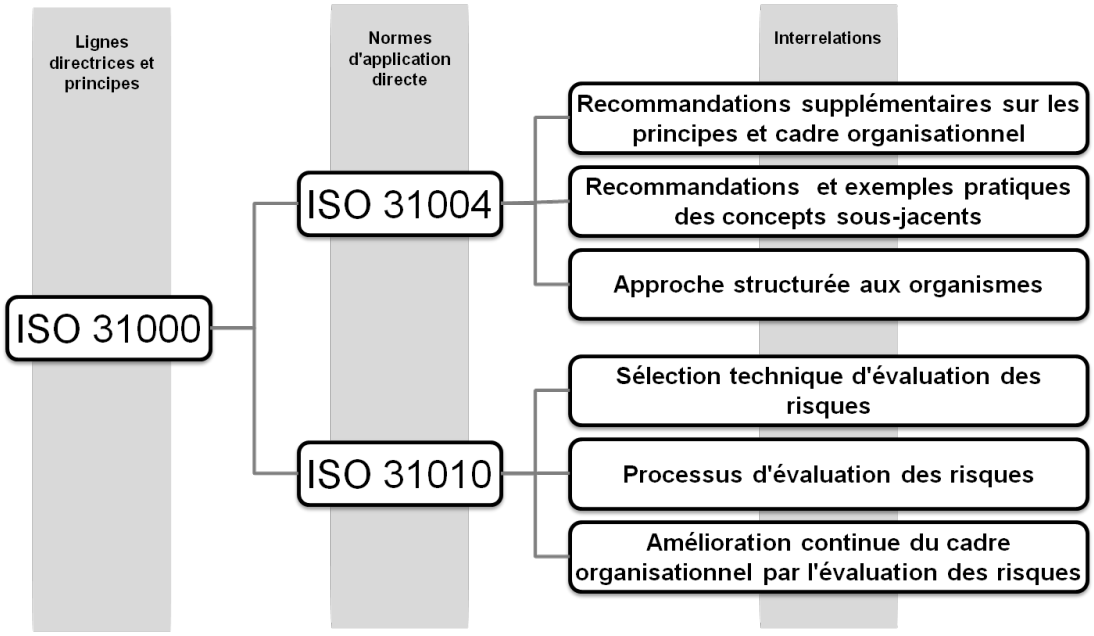

Figure 3 : Lien entre les normes ISO 31000, 31004 et 31010 [source : auteurs]

Les freins au management du risque

Le management du risque comme le préconise les normes est une approche plus facilement mise en œuvre par les grands organismes, ce qui ne semble pas le cas, d'après une étude de l'ISO Focus+, pour les PME (Petites et Moyennes Entreprises), TPE (Très Petites Entreprises) et ETI (Entreprises de Taille Intermédiaire) [12]. Elles auraient, avec les référentiels normatifs, des difficultés telles que :

- de compréhension de la norme ISO 31000 ;
- à élaborer la mise en œuvre du management du risque ;
- à percevoir le rapport coût/bénéfice par rapport aux ressources à mobiliser.

Des outils d'évaluation des risques et des guides existent [13]–[15] et sont disponibles sous différentes formes de support mais aucun ne propose un accompagnement au quotidien et facile au management du risque.

Quand simplicité résonne avec performance

Dans l'objectif de répondre principalement aux besoins de compréhension et d'accompagnement des TPE, PME, et ETI, deux outils simples ont été créés, basés sur la famille des normes ISO 31000. Ils donneront l'avantage à l'utilisateur d'aborder la compréhension du management du risque par l'angle qui lui convient puis de l'introduire dans sa structure [16].

Parmi les nombreux logiciels existants sur internet, il est apparu que deux présentations, l'une sous forme d'une interface « full web » interactive et l'autre sous forme d'une grille d'auto-évaluation sous Excel®, sont les plus pertinentes. Elles permettent de répondre aux besoins des organismes : comprendre rapidement la norme et faciliter la mise en œuvre du management du risque.

Ce sont deux outils simples d'utilisation et offrant une manipulation plus aisée et intuitive que d'autres logiciels comme par exemple Word®, Access® et Visual Basic® (figures 4 et 5).

Logiciel	Téléchargement obligatoire	Ergonomie	Prix	Choix effectué
Word®	Oui	- -	Dans pack office	Interface web
Visual Basic®	Oui	-	Selon licence	
Excel®	Oui	-	Dans pack office	
Scenari	Non	+ + +	Version libre	

Figure 4 : Comparaison des logiciels pour l'interface web [source : auteurs]

Logiciel	Maîtrise	Ergonomie	Prix	Choix effectué
Word®	+ + +	- -	Dans pack office	Auto diagnostic
Access®	+	+ +	Selon licence	
Excel®	+ + +	+ + +	Dans pack office	
Sphinx	-	+ +	Selon licence	

Figure 5 : Comparaison des logiciels pour l'autodiagnostic [source : auteurs]

Une interface web ergonomique pour faciliter la compréhension de l'ISO 31000

Cette interface développée à partir du logiciel SCENARIChain© [17] permet d'accéder à un résumé de chaque élément clé des trois articles de recommandations (3, 4 et 5) de la norme ISO 31000 :

- Article 1 « Domaine d'application » (sans recommandation) ;
- Article 2 « Termes et définitions » (sans recommandation) ;
- **Article 3 « Principes du management du risque »** : énonce les principes auxquels adhérer pour un management de risque efficace ;
- **Article 4 « Cadre organisationnel »** : présente le mandat et l'engagement, la conception du cadre organisationnel, la mise en œuvre, la surveillance et revue et l'amélioration continue ;
- **Article 5 « Processus »** : présente la communication et concertation, l'établissement du contexte, l'appréciation du risque, le traitement du risque, la surveillance et revue, et l'enregistrement du processus.

Les fenêtres de navigation génèrent des représentations graphiques avec les items détaillés comme : les définitions, les acteurs, les données d'entrée et de sortie, les recommandations, les supports en lien avec les informations recherchées. La figure 6 illustre la représentation graphique de l'article 4 « Cadre organisationnel » avec un zoom sur une de ses étapes « Mandat et engagement ».

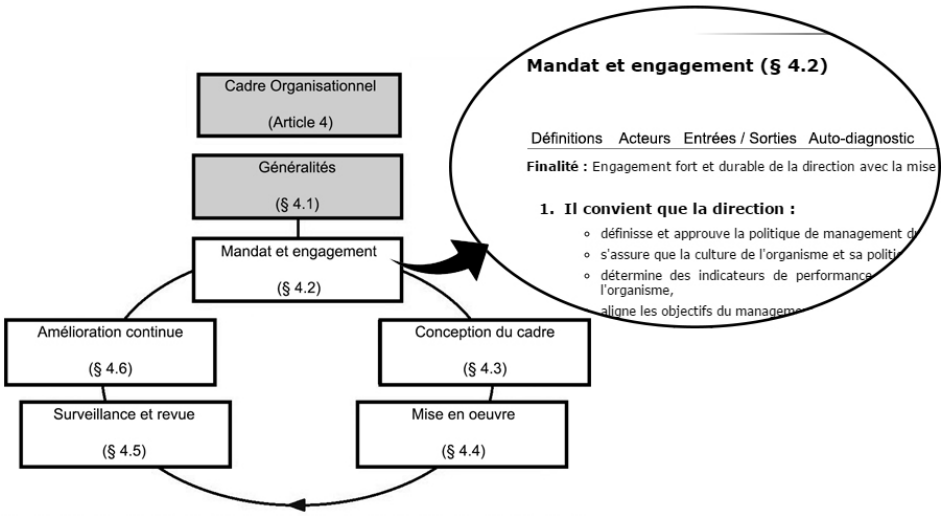

Figure 6 : Représentation graphique des étapes de l'article 4 de la norme ISO 31000 [16]

Le lecteur va se déplacer librement dans l'arborescence créée, revenir à l'étape précédente ou passer à une autre aisément pour aboutir à une compréhension simplifiée de la norme. Il va pouvoir ainsi intégrer plus rapidement les recommandations de mise en œuvre de management du risque au sein de son organisation.

Un outil d'autodiagnostic interactif pour une évaluation en quelques clics

L'autodiagnostic situe l'organisme sur sa stratégie de management des risques à partir des niveaux de respect des recommandations présentes dans les articles 4 et 5. Il lui sert aussi à évaluer périodiquement l'évolution de cette stratégie de même que ses points forts et critiques tout en gardant une traçabilité. L'outil rappelle également les principes évoqués dans l'article 3 de la norme auxquels l'organisme devrait adhérer.

L'autodiagnostic se fait via une check-list sous forme d'un tableau automatisé d'Excel® pour privilégier simplicité et rapidité. Il peut être réalisé individuellement ou collectivement, cette dernière option permet de diminuer l'incertitude, limiter la subjectivité individuelle, partager l'information et améliorer la communication au sein de l'organisation.

L'ensemble des recommandations sont synthétisées en seulement 109 critères. L'évaluation de ces derniers suit une cotation en pourcentage de « véracité » sur 4 niveaux paramétrables :

- Faux : L'action n'est pas réalisée ou alors de manière très aléatoire (0%) ;
- Plutôt faux : L'action est réalisée quelques fois de manière informelle (30%) ;
- Plutôt vrai : L'action est formalisée et réalisée de manière assez convaincante (70%) ;
- Vrai : L'action formalisée est réalisée, améliorée et tracée (100%).

Les pourcentages des critères évalués sont ensuite moyennés automatiquement pour générer un niveau de respect des recommandations sur chacune des 12 étapes (sous articles) des articles 4 et 5 :

- Insuffisant : Il est nécessaire de formaliser les pratiques (0 à 14%) ;
- Informel : Il est nécessaire d'assurer la bonne exécution des pratiques (15 à 49%) ;
- Acceptable : Il est nécessaire d'améliorer les pratiques (50 à 74%) ;
- Convaincant : Bravo ! Maintenez et communiquez vos résultats (75 à 100%).

De la même façon, les pourcentages de satisfaction des étapes au sein de chaque article sont moyennés pour donner naissance au pourcentage de satisfaction final de l'article concerné (figure 7).

	Réf.	Items des articles de la norme	Evaluations	Taux %	Libellés des évaluations	Modes de preuve et commentaires
Article	Art .4	Cadre Organisationnel	Acceptable	74%	Respect de niveau 3 : Il est nécessaire d'améliorer les pratiques	
Etape	4.2	Mandat et engagement	Acceptable	66%	Respect de niveau 3 : Il est nécessaire d'améliorer les pratiques	
Critères	1	La direction définit et approuve la politique de management du risque	Plutôt Faux	30%	Niveau 2 : L'action est réalisée quelques fois de manière informelle.	
	2	La direction s'assure que la culture de l'organisme et sa politique de management du risque sont en phase	Plutôt Faux	30%	Niveau 2 : L'action est réalisée quelques fois de manière informelle.	
	3	La direction détermine des indicateurs de performance du management du risque cohérents avec les indicateurs de performance de l'organisme	Choix FAUX Plutôt Faux Plutôt Vrai VRAI	0%	Niveau 1 : L'action n'est pas réalisée ou alors de manière très aléatoire.	

Figure 7 : Extrait de la grille d'évaluation de l'autodiagnostic du management du risque [16]

L'outil génère en temps réel des résultats synthétiques en fonction des évaluations réalisées (figure 8). Les onglets {Résultats Article 4}, {Résultats Article 5} et {Résultat Global} présentent les synthèses de façon simple et communicante afin de permettre à n'importe quel acteur d'identifier au premier coup d'œil les points critiques. Dans une logique de progrès, l'outil d'autodiagnostic intègre un espace dédié aux plans d'actions. Ce dernier permet de tracer les différentes ressources à mobiliser, les planifications et objectifs, les mesures de succès et les résultats obtenus.

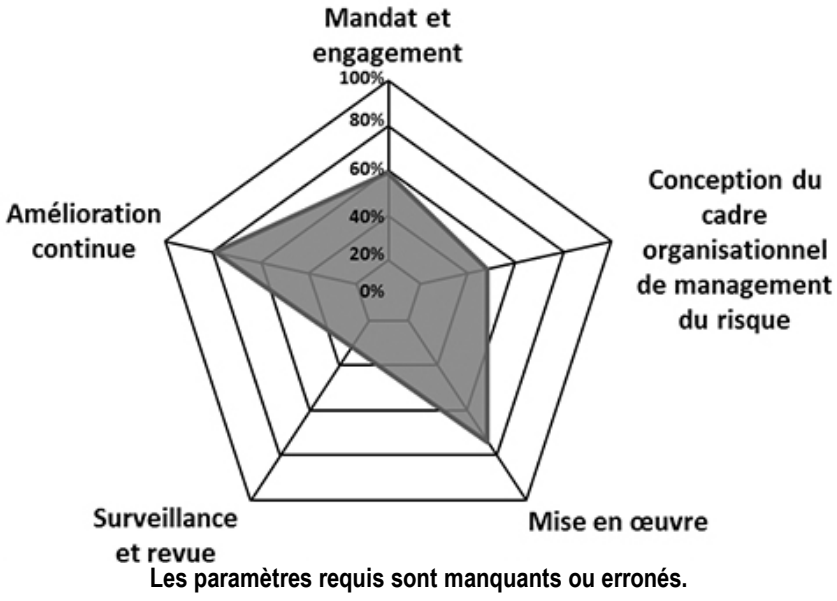

Figure 8 : Synthèse de l'évaluation de l'article 4 « Cadre organisationnel » de l'ISO 31000 [16]

Conclusion

L'évolution du marché pousse les organismes à anticiper leurs risques pour rester au premier plan et être performants. Les grands organismes se sont rendus compte de la nécessité de gérer les risques dans leur globalité et à tous les niveaux de leurs processus d'activité. Face aux besoins exprimés sur la manière de manager les risques, les instances internationales de normalisation ont répondu par la publication de la norme ISO 31000 « Management du risque – Principes et lignes directrices ».

Néanmoins, de nombreuses TPE, PME et ETI ne perçoivent ni l'intérêt d'adopter un management du risque, ni ses bénéfices à court, moyen et long terme. Afin de leur faciliter la mise en œuvre de la norme ISO 31000 et gagner du temps, deux outils sont proposés :

- Le premier outil est une interface disponible sur internet. Il présente une vue d'ensemble de la norme ISO 31000 et donne la latitude à l'utilisateur de l'aborder dans l'ordre qui lui convient.
- Le deuxième outil est une grille d'autodiagnostic téléchargeable et adaptable, qui permet d'évaluer la pertinence du cadre organisationnel et l'efficacité du processus du management du risque.

Ces deux outils permettent d'appréhender de manière interactive le contenu de cette norme, de visualiser le niveau de maîtrise des risques ainsi que son évolution. Ils offrent une démarche proactive à adopter pour réduire les risques à tous les niveaux des processus de l'organisation.

Intégrer la maîtrise du risque au processus de management, réduire les menaces en les anticipant et saisir les opportunités, est une démarche dont la mise en œuvre facilite l'atteinte des objectifs fixés. Elle permet aux organismes d'améliorer quotidiennement et durablement leur performance notamment économique et sociale.

Déclaration d'intérêts

Les auteurs déclarent ne pas avoir de conflits d'intérêts en relation avec cet article.

Références bibliographiques

[1] « Conséquences sanitaires de la catastrophe d'AZF ». Ed. Institut de veille sanitaire, www.invs.sante.fr, oct-2015.

[2] N. Couderc et O. Montel-Dumont, « Les politiques économiques à l'épreuve de la crise ». Ed. La Documentation Française, les Cahiers Français, Vol 359, nov-2010.

[3] K. Mohsen-Finan, « Le printemps arabe reconfigure l'environnement du Maghreb ». Ed. IRIS, www.iris-france.org, oct-2014.

[4] « Fièvre hémorragique virale (FHV) à virus EBOLA ». Ed. Institut de veille sanitaire, www.invs.sante.fr, févr-2015.

[5] P. Anglard, J. Lacroix, et F. Lau, « Analyse et gestion des risques dans les grandes entreprises : impacts et rôle pour la DSI ». Ed. CIGREF, www.cigref.fr, oct-2007.

[6] « NF ISO 31000 Management du risque - Principes et lignes directrices ». Edition Afnor, www.afnor.org, janv-2010.

[7] J.-D. Darsa, *La gestion des risques en entreprise : Identifier, comprendre, maîtriser. Les risques économiques, stratégiques, financiers, opérationnels, juridiques, informatiques*, 3éme édition. Ed. GERESO, 2013.

[8] J.-D. Darsa, *365 risques en entreprise - Une année en risk management*, 2éme édition. Ed. GERESO, 2014.

[9] Federation of European Risk Management Associations (FERMA), « Keys to Understanding the Diversity of Risk Management in a Riskier World », Editions FERMA, Benchmarking Survey 2012 6th Edition, www.ferma.eu, Bruxelles, oct. 2012.

[10] « FD ISO 31004 Management du risque - Lignes directrices pour l'implémentation de l'ISO 31000 ». Edition Afnor, www.afnor.org, févr-2014.

[11] « NF EN 31010 Gestion des risques Techniques d'évaluation des risques ». Edition Afnor, www.afnor.org, juill-2010.

[12] R. Weissinger, « Management du risque - L'aide des normes ISO », *ISO Focus+, www.iso.org/isofocus+*, vol. 4, n° 2, p. pages 19 à 21, févr-2013.

[13] « OiRA : Outils d'évaluation des risques ». Edition Agence Européenne pour la sécurité au travail, www.osha.europa.eu/fr, nov-2015.

[14] « Guide d'auto-évaluation des risques professionnels ». Editions Carsat Alsace Moselle, www.carsat-alsacemoselle.fr, août-2012.

[15] AIRMIC, Alarm, et IRM, « A structured approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000 ». Ed. AIRMIC www.airmic.com, Ed. Alarm www.Alarm-uk.org, Ed. IRM www.theirm.org, 2010.

[16] O. Aby Salami, D. El Haouli, F. Konté, O. Mansour, I. Motte, et B. E. Ouali, « Management du risque performant : Faciliter l'usage de l'ISO 31000 », Université de Technologie de Compiègne, Master Qualité et Performance dans les Organisations (QPO) et Mastère Spécialisé Normalisation, Qualité, Certification, Essai (NQCE), Mémoire d'Intelligence Méthodologique du projet d'intégration, http://www.utc.fr/master-qualite, puis « Travaux » « Qualité-Management » n° 333, janv. 2016.

[17] UTC et KELIS, « SCENARIchain ». Ed. KELIS, www.scenari-platform.org, nov-2015.