Master Qualité et Performance dans les Organisations

QPO12 - Communication professionnelle de projet

2015-2016

# Management du Risque Performant : Faciliter l'usage de l'ISO 31000


***Initiateur du projet : M. Gilbert FARGES***

***Réalisé par :***

***Odile ABY SALAMI – Dina EL HAOULI – Fatimata KONTE***

***Ones MANSOUR – Isabelle MOTTE – Bahaa Eddine OUALI***



*www.utc.fr/master-qualite/ puis « Travaux », « Management qualité », Référence 333*

# Remerciements

Nous tenons à remercier notre tuteur et professeur Monsieur Gilbert FARGES de nous avoir accompagnés et guidés tout au long du semestre pour mener à bien notre projet. Nous le remercions pour son dévouement en matière d'enseignement et le temps qu'il nous a consacré.

Nous remercions de surcroît les professeurs Monsieur Jean-Pierre CALISTE, Monsieur Jean ESCANDE et Monsieur Arnaud DERATHE pour toute la richesse des explications et des conseils qu'ils nous ont apportés.

Nous remercions enfin toutes les personnes qui ont contribué, de près ou de loin, au déroulement de ce semestre dans les meilleures conditions.

# Résumé

Au cours du temps, la multiplication des différents évènements tragiques a démontré l'importance de la gestion adéquate des risques. Désormais, la gestion des risques est un élément indispensable à la survie de tout type d'organisme. Le risque peut être, en effet, pilote de décisions stratégiques, source de nombreuses incertitudes et une menace à la pérennité des activités.

Une approche globale du management du risque permet d'évaluer l'impact de tous les types de risques sur tous les processus, y compris les personnes, les biens et l'environnement. C'est dans cette logique qu'a été publiée la norme ISO 31000 « Management du risque – Principes et lignes directrices». Elle offre une approche structurée et globale de la mise en œuvre du management du risque en entreprise.

De nombreux organismes rencontrent des difficultés face à la mise en œuvre de cette norme. Ce mémoire met à disposition deux outils simples, conviviaux et ergonomiques qui aideront ces organismes à intégrer l'ISO 31000 au sein de leurs organisations.

***Mots-clefs:*** *ISO 31000, management, performance, risque, enjeux, impact, stratégie, outils, autodiagnostic, interface web, évaluation.*

## Abstract

Through the time, the proliferation of different tragic events demonstrated the importance of adequate risk management. Nowadays, risk management is an essential practice for the survival of all types of organizations. The risk may be, in fact, a driver of strategic decisions, it may be a cause of uncertainty and a threat to the sustainability of the organization.

An enterprise-wide approach to risk management enables an organization to consider the potential impact of all types of risks on all processes, including the people, the goods and the environment. In this context was published the international standard, ISO 31000 " Risk management - Principles and guidelines ". It provides a structured and comprehensive approach to the implementation of risk management in companies.

Many organizations face difficulties with the implementation of this standard. This thesis provides two simple, user-friendly and ergonomic tools to help these organizations to integrate ISO 31000 within their organizations.

***Keywords:*** *ISO 31000, management, performance, risk, challenges, impact, strategy, tools, self-diagnosis, web interface, evaluation.*

# Table des matières

REMERCIEMENTS
RÉSUMÉ
TABLE DES MATIÈRES
TABLE DES ILLUSTRATIONS
LISTE DES ABRÉVIATIONS

INTRODUCTION 7
1. ENVIRONNEMENT GÉNÉRAL 8
1.1. Contexte 8
1.2. Enjeux 9
1.3. Le risque en entreprise 10
1.4. Chiffres et benchmarking sur le management du risque 12
1.5. Lien avec les autres normes abordant la notion de risque 16
1.6. Bilan 18
2. CRÉATION D'OUTILS 19
2.1. Présentation des normes relatives au management du risque 20
2.2. Choix des outils 23
3. ABOUTISSEMENT DES OUITLS 25
3.1. L'interface web sous SCENARIChain© 25
3.2. Outil d'Autodiagnostic 28
3.3. Bilan 33
CONCLUSION 34
BIBLIOGRAPHIE 36
LEXIQUE 38
ANNEXES 40

# Table des illustrations

Figure 1 : Les différentes catégories de risque ..... 11
Figure 2 : Évolution du nombre de participants au sondage de FERMA concernant le Risk management ..... 13
Figure 3 : La répartition des participants par secteurs d'activité ..... 13
Figure 4 : Les profils métier des personnes ayant répondu aux questionnaires ..... 14
Figure 5 : Classement des facteurs externes incitant les entreprises au Risk management ..... 14
Figure 6 : Les référentiels du Risk management les plus utilisés par les entreprises ..... 15
Figure 7 : Lien entre les normes ISO 31000, 31004 et 31010 ..... 22
Figure 8 : Relation entre les principes, le cadre organisationnel et le processus du management du risque ..... 22
Figure 9 : Choix du support pour l'interface web ..... 23
Figure 10 : Choix du support pour l'outil autodiagnostic ..... 24
Figure 11 : Page d'accueil web ..... 25
Figure 12 : Représentation graphiques des trois articles de la norme et son annexe ..... 25
Figure 13 : Représentation graphique de l'article 4 et onglets d'information ..... 26
Figure 14 : Extrait du dernier niveau de l'arborescence ..... 27
Figure 15 : Onglet Mode d'emploi de l'outil autodiagnostic ..... 28
Figure 16 : Extrait de la grille d'évaluation de l'outil autodiagnostic ..... 29
Figure 17 : Aperçu de l'onglet résultat de l'outil autodiagnostic ..... 30
Figure 18 : Aperçu de l'onglet résultat global ..... 31
Figure 19 : Logigramme d'utilisation de l'outil d'autodiagnostic ..... 32
Figure 20 : Documents normatifs à paraître et relatif au management du risque ..... 35

# Liste des abréviations

**AFNOR** : Association Français de Normalisation

**AMRAE :** Association pour le Management des Risques et des Assurances de l'Entreprise

**CN:** Commission de Normalisation

**COSO:** Committee of Sponsoring Organizations

**ETI :** Entreprise de Taille intermédiaire (de 250 à 4999 salariés, CA < 1,5 milliard d'EUR) [1]

**FERMA:** Federation of European Risk Management Association

**IOS (ISO en français)** : International Organisation for Standardization

**ONG** : Organisation Non Gouvernementale

**PME :** Petite et Moyenne Entreprise (< 250 salariés, CA < 50 millions d'EUR) [1]

**SMQ :** Système de Management de la Qualité

**TPE :** Très Petite Entreprise (< à 10 salariés, CA < 2 millions d'EUR) [1]

# Introduction

Le risque n'est pas une découverte du monde moderne. En effet, l'homme l'a intégré naturellement dans son mode de fonctionnement depuis la nuit des temps mais de façon intuitive pour sa sauvegarde.

Le début du XXI$^{ème}$ siècle a été marqué par des événements tragiques (la peur du « bug » de l'an 2000 [2], les attentats du 11 septembre 2001 [3], la crise des subprimes [4] , les soulèvements du monde arabe [5], épidémie du virus « Ebola » [6], …) qui ont bouleversés le quotidien des hommes et ont également fragilisés les interdépendances mondiales.

Cette mondialisation des marchés a mis en évidence les difficultés que rencontrent les organismes à gérer l'environnement incertain et fluctuant les entourant.
Cet environnement est source de risques qui peuvent aussi bien être interne qu'externe aux organismes. Ils peuvent mettre les organismes en péril s'ils n'ont pas anticipé les fluctuations de leur environnement. Les anticiper peut aussi être une force, un atout.

De ce fait, est apparu le terme de « Risk management » qui est une matière assez nouvelle en France sauf pour les entreprises ayant déjà une envergure internationale. Suivant qu'il est utilisé dans le monde de l'entreprise, ou dans le langage courant, il ne revêt pas la même signification. Afin d'en donner une même lecture, l'ISO 31000 [7] a vulgarisé la notion de risque dans le but de la rendre compatible à tout type d'activité et de permettre ainsi une communication avec dialectique commune.

Tout au long de ce mémoire, la norme sera décrypter afin de garantir une lecture conviviale et la mise à disposition des outils vous permettra :

- de vous situer quant à votre gestion actuelle du risque,
- et de vous guider pour intégrer la gestion du risque à tous les niveaux de vos processus.

*«Le monde a commencé sans l'Homme, c'est un fait.*
*Et le risque est qu'il se prolonge sans lui».*

*Laurent Fabius, le 03/10/2015 au forum « Make It Work » organisé par « Libération » à Sciences Po Paris.*

# 1. ENVIRONNEMENT GÉNÉRAL

## 1.1. Contexte

Historiquement et contrairement aux entreprises françaises, les entreprises anglo-saxonnes ont toujours été en avance en matière de risk management. En effet, la première apparition de la gestion des risques « moderne » fut aux États-Unis entre les années 1950 et 1960. Cette gestion étant limitée à cette époque au transfert des risques vers un assureur [8]. Cette notion a évolué pour prendre une importance capitale dans la vie des entreprises depuis les années 2000, en étant de plus en plus intégrée dans la stratégie globale de l'entreprise et en devenant un élément clé pouvant influer sur les principes de l'organisation de l'entreprise.

Les organismes, de par leurs diversités en termes de types, secteurs et tailles (entreprise, gouvernement, ONG, individu, etc.) sont confrontés à des facteurs qui les influencent à l'interne comme à l'externe. L'incertitude générée par ces facteurs, portant sur l'atteinte des objectifs d'un organisme, en constitue le risque. De nos jours, les organismes se trouvent devant deux objectifs qui semblent, à première vue, contradictoires à savoir :

- le développement de l'innovation dans la quête d'offrir un produit meilleur et la conquête de nouveaux marchés d'un côté

- la garantie d'un haut niveau de sécurité et la maîtrise des risques souvent engendrés par tout processus innovant d'un autre.

La précaution est un traitement du risque qui existait avant que l'opinion publique puis la législation ne l'érigent en principe.
En France, depuis le 2 février 1995, la précaution a une définition légale qui est : « L'absence de certitudes, compte-tenu des connaissances scientifiques et techniques du moment, ne doit pas retarder l'adoption de mesures effectives et proportionnées visant à prévenir un risque de dommages graves et irréversibles à l'environnement à un coût économiquement acceptable. » (Loi 95-101 dite loi Barnier).

La norme ISO 31000 constitue une solution efficace pour aider les entreprises à déployer leur approche-risque de façon structurée sans préconiser des moyens opérationnels pour sa mise en œuvre. Cette norme dresse d'intéressantes interrogations de manière à aborder ce sujet complexe qui est la gestion des risques, en ayant comme objectif de fournir des principes et des lignes directrices pour le management du risque en favorisant l'intégration de ce dernier dans le système managérial de l'organisme [9].

## 1.2. Enjeux

Le dictionnaire Larousse [10] donne un éclaircissement du terme enjeu en proposant deux définitions.

1. *Ce que l'on risque dans un jeu, en particulier une somme d'argent et qui revient au gagnant.*

Ici, un terme surprend, le mot jeu. En effet, prendre un risque c'est comme jouer à quitte ou double.

2. *Ce que l'on peut gagner ou perdre dans une entreprise quelconque.*

C'est la probabilité d'un gain ou d'une perte à venir.

Au fil de ce mémoire, la définition du risque selon la norme ISO 31000 sera donnée.

La corrélation des deux définitions, permet de définir l'enjeu comme étant le fait que dans une situation quelconque on peut tout autant gagner que perdre. De plus, l'enjeu se base sur ce qu'on a investi ou on souhaite investir. Cet investissement sera au bénéfice ou au détriment de celui qui a pu investir des éléments tant matériels (financier, propriétés), qu'immatériels (son honneur, son image).

Voici ci-dessous les cinq enjeux majeurs :

- Enjeux techniques
- Enjeux sociétaux
- Enjeux économiques
- Enjeux environnementaux
- Enjeux éthiques

L'ensemble de ces enjeux peut avoir des impacts tant sur la santé que sur la sécurité des parties prenantes (salariés, consommateurs, Etat, …) contraignant les organismes à maîtriser leurs activités de manière efficace et efficiente.

Du fait de l'accentuation du contexte concurrentiel, les organismes doivent savoir mieux maîtriser les coûts, les délais, les spécifications techniques des projets ainsi que leurs incidences sur leur environnement immédiat.

D'autre part, l'impact de l'opinion publique sur les activités des organismes n'est plus en reste car elles peuvent entacher leur image de marque.

Ainsi cerner ses enjeux pourra s'avérer bénéfique du point de vue :

- du respect de l'environnement (ex. préservation des ressources naturelles et des matières premières nécessaires à une activité),
- de la santé et de la sécurité des personnes (ex. limitation du nombre d'accidents de travail),

- de la conformité légale et réglementaire (ex. l'égalité professionnelle en termes de salaires et de promotions, la diversité en entreprise, la lutte contre la corruption, le non-travail des enfants),
- des performances financières et économiques (ex. augmentation du chiffre d'affaires, gain des parts du marché).

La gestion des enjeux revient donc à :

- ✓ Appréhender les risques et les évaluer au mieux
- ✓ Maîtriser les risques en les anticipant et en les encadrant
- ✓ Réagir très rapidement

La prise en compte de la gestion d'un risque doit se faire très en amont. En effet, l'organisme pourra anticiper les risques et sensibiliser l'ensemble de son organisation aux éventuels bouleversements pouvant mettre en péril sa pérennité et/ou sa stabilité. L'organisme peut : soit être conscient qu'il ne maîtrise pas totalement son environnement, soit le risque ne fait pas l'objet de toutes ses attentions.

L'enjeu est indissociable du risque car ils sont interdépendants. Manager le risque est déjà un enjeu en soi car il permet de reconnaître les défaillances pouvant apparaître. De plus, la mesure du niveau du risque présent ou potentiel sera meilleure.

Au cas d'espèce, l'enjeu environnemental encourage une entreprise à prendre en compte dans son processus d'achat les éléments pouvant causer un préjudice à l'écosystème ex : pollution, dégradation des ressources naturelles.

## 1.3. Le risque en entreprise

### 1.3.1. La définition du risque

Selon la norme ISO 31000 : « Les organismes de toutes sortes sont confrontés à des facteurs et des influences internes et externes, de sorte qu'ils ignorent s'ils vont atteindre ou dépasser leurs objectifs et, si oui, à quel moment et dans quelle mesure. L'incidence de cette incertitude sur l'atteinte des objectifs d'un organisme constitue le risque. »

### 1.3.2. Les critères d'évaluation d'un risque

Selon Jean-David DARSA [11], [12], le risque peut être évalué grâce à 3 critères principaux :

1. La détectabilité : mesure de la capacité d'un système organisationnel à détecter le risque entrant.
2. La sévérité : chiffrage de l'impact (conséquence) du risque, en cas d'émergence
3. L'occurrence appelée aussi la vraisemblance : mesure de la probabilité d'apparition du risque identifié dans le système.

La multiplication de ces trois critères permet de calculer un facteur risque qui constitue un critère de qualification pertinent du risque et de son enjeu à traiter.

### 1.3.3. Les différentes catégories de risque

Il existe une multitude de risques qui peuvent menacer et mettre en cause la pérennité ainsi que l'atteinte des objectifs d'une organisation. Afin de les gérer de manière efficace, chaque organisme doit identifier et classer ses risques en fonction de ses enjeux prioritaires.

Pour chaque secteur d'activité existe un faisceau spécifique de risques susceptibles d'impacter les organismes, de manière propre et spécifique. Et, pour chaque organisme du même secteur d'activité, le spectre des risques à couvrir sera spécifique, en fonction de son histoire, de sa taille, de son ancienneté, de son organisation, de son mode de fonctionnement, de son encadrement, etc.

De même, chaque processus et sous-processus traduisant une activité de l'organisme va être aussi exposé à un spectre de risques spécifiques, plus ou moins sévères.

D'une manière exhaustive, Jean-David DARSA a déterminé 11 principales catégories de risques (*voir Annexe A*).

| Catégorie de risques | Exemples |
|---|---|
| **Risques géopolitiques** | Blocus économique, attentats, guerres, climat insurrectionnel… |
| **Risques économiques** | Inflation, évolution de la demande, des besoins, des marchés… |
| **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** | Risques engendrés par les infrastructures, les énergies, les cycles de production… |
| **Risques industriels** | Risques liés aux activités de fabrication, de transformation… |
| **Risques juridiques** | Contrefaçon, responsabilité pénale du dirigeant… |
| **Risques informatiques** | Risques liés aux matériels, aux logiciels, aux applications, aux infrastructures réseaux… |
| **Risques sociaux ou psychosociaux** | Perte d'homme clé, mal-être, stress, harcèlement sexuel, suicide… |
| **Risques d'image ou de réputation** | Contrefaçon, rumeurs, concurrence déloyale, espionnage industriel… |
| **Risques de knowledge management** | Perte de connaissance et de savoir-faire |

**Figure 1 : Les différentes catégories de risque [11]**

## 1.4. Chiffres et benchmarking sur le management du risque

### 1.4.1. Les associations traitant de la gestion du risque

Il est intéressant de savoir qu'il existe aujourd'hui, dans plusieurs pays, des associations qui s'occupent du management et de la gestion des risques. Ces associations rassemblent des acteurs privés et/ou publiques qui concourent à la maîtrise des risques dans les organisations auxquelles ils appartiennent.

En France, par exemple, l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) promeut les travaux en matière de gestion de risques au niveau national mais aussi international. D'une part, elle a pour principaux objectifs de développer et faire évoluer les méthodologies de gestion des risques et d'autre part, aider ses membres à respecter les standards les plus exigeants concernant la maîtrise des risques.

Cette association fait partie d'une organisation qui rassemble toutes les autres associations des pays européens autour de la gestion des risques. C'est la fédération des associations européennes du management du risque FERMA (Federation of European Risk Management Associations). Elle permet de coordonner les travaux du management du risque des associations y adhérant, et optimise les effets de ces dernières en dehors de leurs frontières nationales au niveau européen.

### 1.4.2. Le management du risque en Europe

En 2012, une étude sur les pratiques de Risk Management en Europe a été réalisée par la fédération européenne FERMA (Federation of European Risk Management Associations) en collaboration avec AXA Corporate Solutions et Ernst & Young [13].

Le sondage, composé de 41 questions, a reçu 809 réponses représentant 20 pays. Ses objectifs sont les suivants :

- Analyser l'évolution du Risk Management depuis 2010
- Déterminer le niveau de maturité des pratiques de Risk Management dans les entreprises européennes
- Illustrer le lien entre le niveau de performance des entreprises et le niveau de maturité du Risk management
- Comprendre les enjeux futurs du Risk Management

Le nombre de réponses à ce type de sondage a augmenté depuis 2002, ce qui suggère que les organismes deviennent de plus en plus intéressés et familiarisées avec le Risk Management.

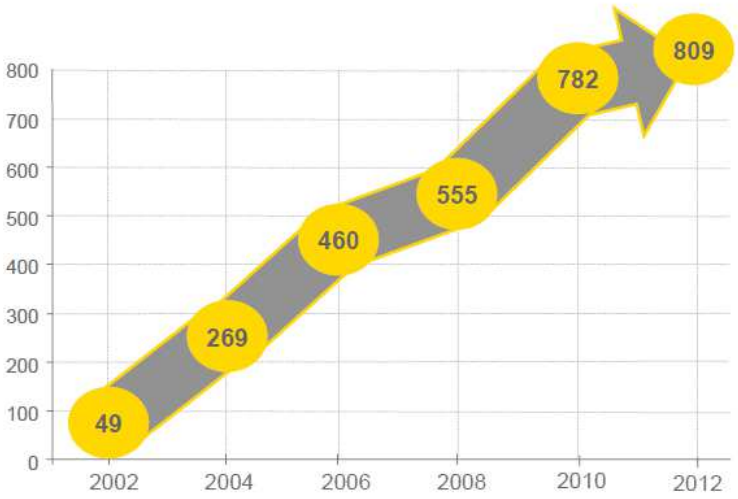


**Figure 2 : Évolution du nombre de participants au sondage de FERMA concernant le Risk management [13]**

Les données ont montré que les participants ayant répondu ont des profils variés et appartiennent à des secteurs différents. Le management des risques concernent donc tous les organismes de tous types et de toutes tailles.

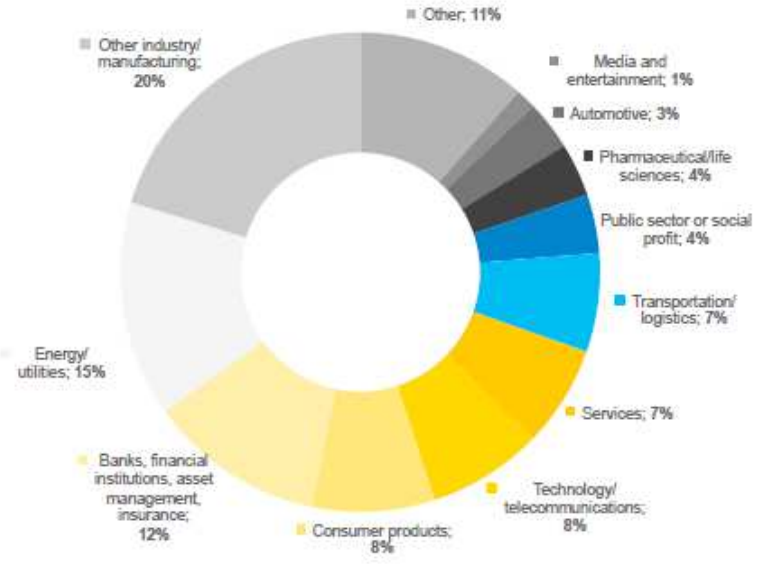


**Figure 3 : La répartition des participants par secteurs d'activité [13]**

72% des personnes, qui ont rempli le questionnaire, sont en charge du Risk Management et/ou de l'assurance.

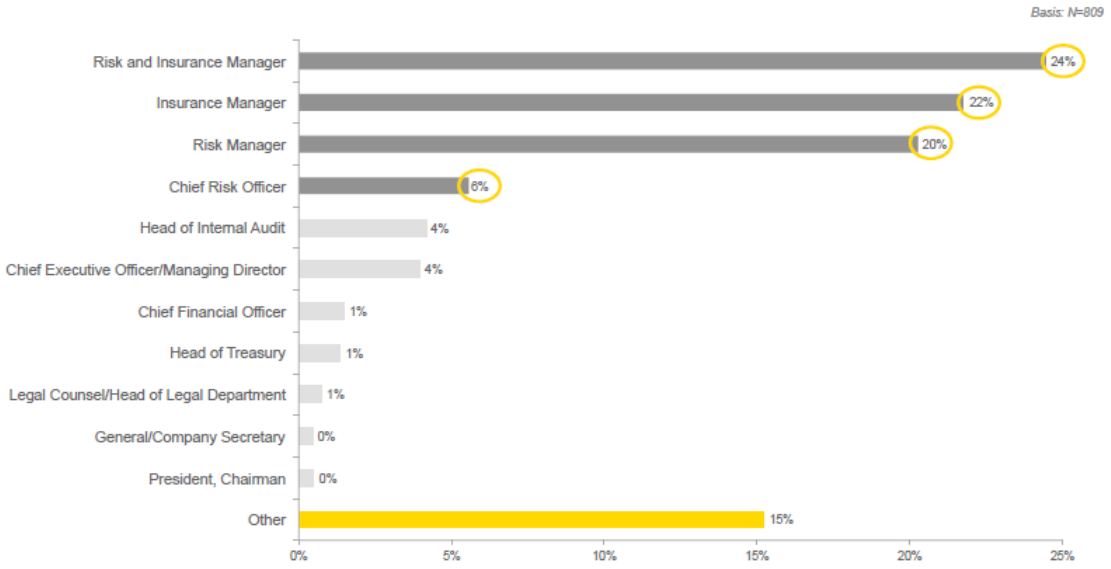


**Figure 4 : Les profils métier des personnes ayant répondu aux questionnaires [13]**

Le questionnaire, interrogeant les entreprises sur les facteurs externes qui les incitent à pratiquer le Risk Management, a révélé que les exigences de conformité, réglementaires et légales sont les facteurs primaires. Il est à remarquer que la responsibilité sociétale est davantage prise en compte par rapport aux évènements catastrophiques.

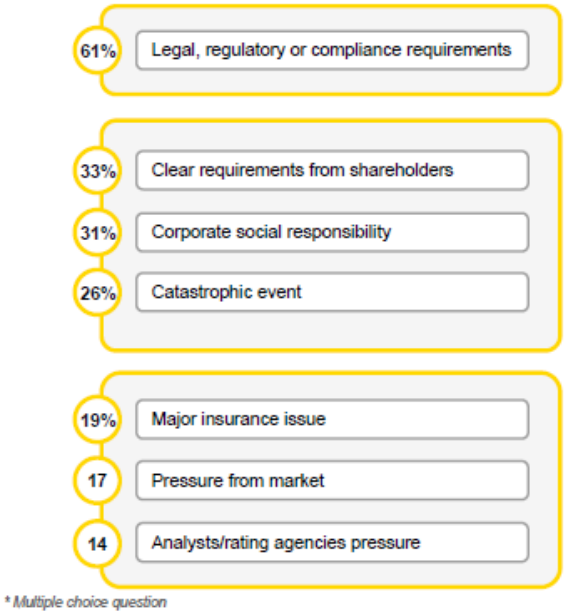


**Figure 5 : Classement des facteurs externes incitant les entreprises au Risk management [13]**

Les participants ont été également interrogés sur quel référentiel ils se basent pour appliquer le Risk Management. Le graphe ci-dessous montre que 37% des entreprises se basent sur le référentiel interne de leur entreprise et non pas sur un référentiel standard comme COSO 2, ISO 31000 ou les référentiels nationaux de Risk Management. Par contre,

en comparant les données de 2012 avec ceux de 2010, il a été noté que la norme ISO 31000 devient de plus en plus utilisée (25% en 2012 au lieu de 13% en 2010).

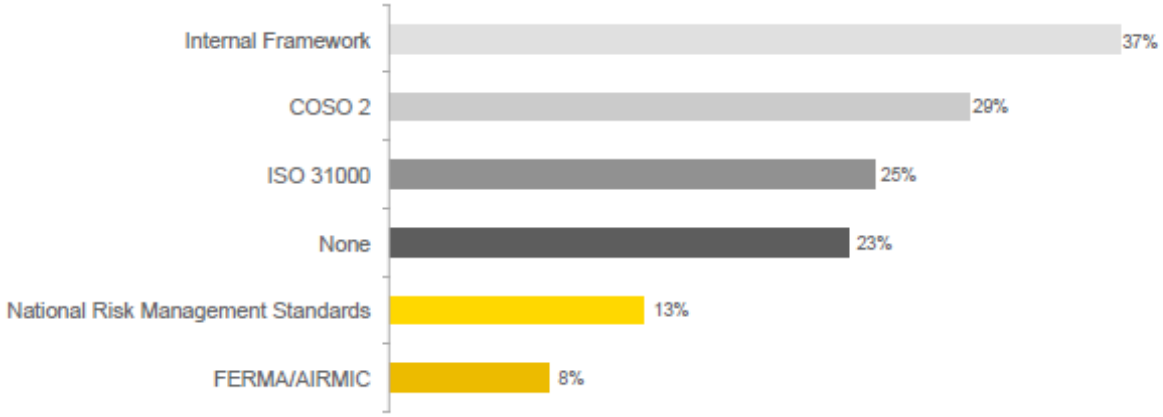


**Figure 6 : Les référentiels du Risk management les plus utilisés par les entreprises [13]**

Les participants ont été ensuite amenés à classifier les risques selon leur importance. Les résultats ont montré qu'en 2012, les cinq risques les plus importants selon les entreprises sont :

- Les risques liés à la compétitivité, les clients, les partenaires et la stratégie
- Les risques liés à la conformité et à la législation
- Les risques financiers
- Les risques liés à la réputation
- Les risques liés au planning et à l'exécution

### 1.4.3. Le référentiel COSO 2

Comme il a été constaté dans les données ci-dessus, le référentiel COSO 2 est actuellement le référentiel le plus appliqué par les entreprises européennes en matière de management des risques. Qu'est-ce-que le référentiel COSO 2 ?

A l'origine, en 1985, cinq associations professionnelles aux États-Unis, se sont alliées pour établir une Commission Nationale qui se consacre aux fraudes financières. Suite à de nombreux scandales aux États-Unis, la commission a mis en place, en 1992, un cadre commun de contrôle interne appelé COSO (Committee Of Sponsoring Organizations). En 2004, la commission élargit le périmètre de ses réflexions et élabore un nouveau référentiel COSO 2 qui est axé davantage sur le processus de management des risques en entreprise.

Ce référentiel a donc été mis en place avant l'ISO 31000 ce qui peut expliquer le fait qu'il est plus utilisé par les entreprises. En revanche, il a été montré que de nombreuses organisations ont rencontré des difficultés à mettre en place le référentiel COSO.
L'ISO 31 000 offre une approche rationalisée qui est plus facile à mettre en œuvre. Il est basé sur un processus de gestion qui s'adapte à chaque organisation et qui s'intègre dans la gestion préexistante. Le modèle COSO, basé sur le contrôle de la conformité, est par contre plus difficilement exploitable pour la gestion de risque global.

## 1.5. Lien avec les autres normes abordant la notion de risque

Le management du risque est souvent évoqué de manière partielle ou globale dans d'autres normes comme dans la nouvelle version 2015 de l'ISO 9001 [14] et de l'ISO 14001 [15]. Il semble judicieux de faire le lien entre ces différentes normes et la norme ISO 31000 afin de guider les organismes à intégrer ce management de façon adéquate dans le cadre de leur application. Cette partie est donc dédiée à tout utilisateur ayant des interrogations sur la façon d'utiliser la norme ISO 31000 à d'autres fins normatives.

### 1.5.1. L'ISO 13485 et le management du risque

Dans sa partie « 7. Réalisation du produit », la norme 13485 [16], qui énonce les exigences relatives au système de management de la qualité dans le cas des dispositifs médicaux, précise que l'organisme doit établir des exigences documentaires relatives au management des risques tout au long du processus de réalisation du produit. De ce fait, tout organisme fournissant des dispositifs médicaux et des services associés est dans l'obligation d'intégrer un certain management de risque dans son organisation afin d'être conforme à cette norme. Toutefois, le recours à la norme ISO 31000 ne permettra pas de répondre totalement aux exigences de la norme 13485 puisqu'il existe une norme plus spécifique et plus adaptée à ce type de management. C'est la norme ISO 14971 qui s'applique à la gestion des risques aux dispositifs médicaux. Elle permet aux fabricants d'identifier les phénomènes et les situations dangereux associés aux dispositifs médicaux, d'évaluer et de maîtriser ce type de risques.

Il est donc recommandable d'utiliser la norme ISO 14971 afin d'intégrer un management des risques adapté selon la norme ISO 13485.

### 1.5.2. L'ISO 9001:2015 et le management du risque

Récemment publiée, la nouvelle norme ISO 9001 version 2015 [14], relative au système de management de la qualité, incite les organismes à prendre en compte les risques et les opportunités associés à leur contexte et à leurs objectifs à tout moment du processus de décision et à tout niveau de leur organisation. Cette approche par les risques est évoquée à plusieurs moments dans le contenue de la norme ISO 9001, notamment dans le paragraphe « 0.3.3. Approche par les risques » et « 6.1. Actions à mettre en œuvre face aux risques et opportunités ». Tout organisme, pour se conformer à cette norme, doit déterminer les risques et mettre en œuvre des actions face à ces derniers. Néanmoins, la norme précise qu'il n'existe pas d'exigences concernant les méthodes formelles de management du risque ou un processus de management de risque documenté. L'organisme peut choisir d'appliquer le référentiel ou la méthode la plus adapté à son organisation. Il peut même opter pour un management de risque plus étendue que n'exige la norme.

Afin de répondre aux exigences de la norme ISO 9001 en ce qui concerne l'approche par les risques, l'organisme peut se baser sur la norme ISO 31000. Elle lui permet de :

- Définir ses objectifs et sa raison d'être
- D'établir le contexte interne et externe de l'organisation
- D'évaluer les risques ayant un impact sur l'atteinte des objectifs

Si toutefois, l'organisme souhaite plus approfondir son évaluation de risques et se concentrer sur le traitement de ses derniers, il peut faire recours directement à la norme ISO 31010 qui va le guider à choisir les méthodes d'évaluation de risques les plus adaptées à son organisation.

### 1.5.3. L'ISO 14001:2015 et le management des risques

De la même façon, la nouvelle version de la norme 14001 [15] relative au système de management environnemental, intègre une approche par les risques. Elle permet à un organisme d'employer un même raisonnement fondé sur le risque pour intégrer son système de management environnemental aux exigences d'autres systèmes de management. Pour ce faire, l'organisme doit déterminer les risques et les opportunités liés à :

- Ses aspects environnementaux
- Ses obligations de conformité
- Ses autres enjeux et exigences identifiés

La prise en compte de ces risques permet de :

- Donner l'assurance que le système de management environnemental peut atteindre les résultats escomptés
- Prévenir ou réduire les effets indésirables
- S'inscrire dans une dynamique d'amélioration continue

Pour être conforme à l'ISO 14001, l'organisme doit aussi planifier les actions pour traiter les risques et évaluer l'efficacité de ses actions. Cette norme n'impose pas non plus des exigences pour un management formel du risque. Il revient à l'organisme de choisir la méthode qu'il utilisera pour déterminer les risques.

Comme pour la norme ISO 9001, tout organisme souhaitant se baser sur un référentiel pour faire une évaluation de risques adaptée dans le cadre de l'ISO 14001, peut faire recours à la norme ISO 31010 et si le souhaite à la norme 31000 pour un management du risque plus global.

### 1.5.4. L'ISO 26000:2010

Cette norme met en avant les bénéfices de la responsabilité sociétale pour une organisation. En effet, elle favoriserait la prise de décision plus éclairée fondée sur une meilleure appréhension des opportunités et des risques liés au fait de ne pas assumer sa responsabilité sociétale.

La norme ISO 26000 [17] aborde la notion de risque sous différents angles en évoquant des risques liés :

- ✓ aux droits de l'Homme,
- ✓ aux conditions de travail,
- ✓ à l'environnement,
- ✓ à la loyauté des pratiques,
- ✓ aux consommateurs, …

Une organisation souhaitant s'engager auprès de la société doit prendre en compte tous les risques liés à son activité. Pour cela elle doit identifier, analyser, éviter et atténuer les différents risques. Afin de réaliser cela, cette organisation peut se baser sur la norme ISO 31000 pour la partie évaluation du risque. Puis s'appuyer sur la norme ISO 31010 qui l'aidera à adopter des méthodes et des techniques d'évaluation de risques les plus adaptés à son organisation.

## 1.6. Bilan

Il est nécessaire pour tout organisme désireux de rester dans la course et voir même désireux d'avoir une longueur d'avance, qu'il identifie dans un premier temps les enjeux pouvant impacter directement son activité et ensuite identifier les risques pouvant en découler.
L'anticipation sera une valeur positive tant financière qu'intellectuelle car les membres de l'organisme ayant anticipé le risque ne seront pas pris au dépourvu et agiront au mieux pour les intérêts de l'organisation.

L'ISO 31000 est un fil d'Ariane qui vous sera simplifié afin de vous en faciliter l'exploitation.

Pour ce faire, les normes ISO 31004 [18] et 31010 [19] serviront de base pour élaborer des outils simples et conviviaux d'aide à l'intégration de l'ISO 31000.

## 2. CRÉATION D'OUTILS

Les normes relatives au management du risque sont destinées aux divers intervenants dans la gestion de management des risques à savoir :

- Les personnes en charge de la mise en place des activités de management des risques au sein des organismes
- Les personnes définissant des pratiques
- Les personnes chargées de gérer des risques particuliers
- Les personnes chargées d'évaluer les pratiques

Le management du risque est une approche comprise par les grands organismes qui ont la capacité de se faire aider par des services internes mais aussi par des prestataires en conseil spécialisés dans l'accompagnement pour la mise en œuvre de démarche qualité.
Des études portant sur l'utilisation des normes par les TPE, PME et ETI révèlent les nombreuses difficultés rencontrées par ces dernières [20] :

- sensibilisation limitée ou inexistante aux normes et à leur importance,
- connaissance limitée ou inexistante des normes pertinentes et de la manière de se les procurer,
- compréhension limitée ou inexistante des normes, et difficultés lors de leur mise en œuvre.

L'objectif est de mettre à disposition des organismes type TPE, PME et ETI, des outils simples de compréhension de la démarche à suivre pour la mise en place du management du risque à tous les niveaux de leurs structures (ou sur une partie suivant la volonté et les besoins de ces dernières). En effet, disposant souvent de moins de temps et de capacité à faire appel à des aides extérieures, elles se retrouvent souvent seules devant l'interprétation de ces normes qui nécessitent une lecture approfondie pour en comprendre tout l'intérêt mais aussi une méthodologie pour parvenir, à terme, à la maîtrise du management du risque.

Il est important que ces outils facilitent l'intégration à n'importe quels niveaux des différentes étapes du management du risque afin que chaque organisme puisse se positionner par rapport à ses besoins et ses capacités. Par exemple, une option pourrait consister à introduire des critères de risque lors de la planification d'un nouveau projet important, ce qui permettrait aux personnels de se familiariser avec les concepts du management du risque et d'acquérir l'expérience voulue. Ces outils tentent d'apporter une lecture simple de la capacité à intégrer les risques et donc d'avoir de l'anticipation par rapport à l'avenir même si le risque, comme il sous-entend, reste une incertitude à venir. Incertitude qui peut être négative si non identifiée mais positive si identifiée, anticipée, prévue et encadrée.

## 2.1. Présentation des normes relatives au management du risque

Actuellement trois normes traitent du management du risque. L'ISO 31000 évoque les principes généraux du management du risque. L'ISO 31004 et 31010 sont, quant à elles, des supports de l'ISO 31000. Ci-après, leur contenu en quelques lignes.

### 2.1.1. Norme ISO 31000:2009, Management du risque – Principes et lignes directrices

Cette norme énonce les principes et lignes directrices pour toute forme de risque rencontrée en organisation. L'ISO 31000 définit le risque comme « l'effet de l'incertitude sur l'atteinte des objectifs ». L'application de cette norme donne la possibilité aux organismes d'atteindre de manière significative leurs objectifs, de saisir de nouvelles opportunités et de faire face aux éventuelles menaces.

Toute organisation peut intégrer le management des risques dans son système. Cependant cette norme n'a pas vocation à servir de base à une certification.

La mise en œuvre d'ISO 31000 permet, par exemple, à un organisme :

- D'augmenter la probabilité que les objectifs seront atteints
- D'encourager un management proactif
- De prendre conscience de la nécessité d'identifier et de traiter le risque à travers tout l'organisme
- D'améliorer l'identification des opportunités et des menaces
- De se conformer aux obligations légales et réglementaires, ainsi qu'aux normes internationales
- D'améliorer l'information financière
- D'améliorer la gouvernance
- D'accroître l'assurance et la confiance des parties prenantes
- D'établir une base fiable pour la prise de décision et la planification
- D'améliorer les contrôles
- D'allouer et d'utiliser efficacement les ressources pour le traitement du risque
- D'améliorer l'efficacité et l'efficience opérationnelle,
- De renforcer les performances en matière de santé et de sécurité, ainsi que de protection environnementale
- D'améliorer la prévention des pertes et le management des incidents
- De minimiser les pertes
- D'améliorer l'apprentissage organisationnel
- D'améliorer la résilience organisationnelle (PCA)

### 2.1.2. Norme ISO 31004:2014, Lignes directrices pour l'implémentation de l'ISO 31000

Cette norme a pour objectif d'aligner aisément au sein des organisations les pratiques de leur management du risque avec les principes d'ISO 31000. Un rapport technique est intégré à cette norme (ISO/TR 31004). Il propose aux organismes des lignes directrices de management efficace du risque par la mise en œuvre de l'ISO 31000:2009 par la détection, la compréhension et la gestion des risques. Il est destiné à être utilisé par ceux qui, au sein des organismes prennent les décisions qui influent sur la réalisation de leurs objectifs et ceux qui fournissent aux organismes, conseils et accompagnement en matière de management du risque. Il s'applique à tous types d'activités et à toutes les composantes de tous les organismes.

C'est une approche structurée et adaptable aux différentes organisations.

### 2.1.3. Norme ISO 31010:2009, Gestion des risques – Techniques d'évaluation des risques

Cette norme est axée sur l'évaluation des risques, qui donne aux décideurs un meilleur éclairage des risques pouvant gêner la réalisation des objectifs et leur permet d'évaluer l'adéquation et l'efficacité des contrôles déjà mises en place. Cette norme traite des concepts de l'évaluation des risques, des processus et de la sélection des techniques d'évaluation des risques. Elle permet de se poser des questions pertinentes sur le processus du management des risques telles que :

- Que se passe-t-il et pourquoi ?
- Quelles sont les conséquences ?
- Quelle est la probabilité d'occurrence des risques ?
- Existe-t-il des facteurs permettant de limiter la conséquence du risque ou de réduire sa probabilité d'occurrence ?

Les responsables chargés de l'évaluation des risques doivent être informés des éléments suivants :

- Le contexte et les objectifs de l'organisation
- L'étendue et le type de risques tolérables et la manière dont doivent être traités les risques inacceptables
- La manière dont l'évaluation des risques est intégrée dans les processus de l'organisation
- Les méthodes et techniques à utiliser pour évaluer les risques
- Le rapporteur, la responsabilité et l'autorité en matière d'évaluation des risques
- Les ressources disponibles pour évaluer les risques
- La manière dont l'évaluation des risques sera rapportée et examinée

### 2.1.4. Lien entre les 3 normes

Le lien entre les trois normes peut se résumer suivant cette représentation :

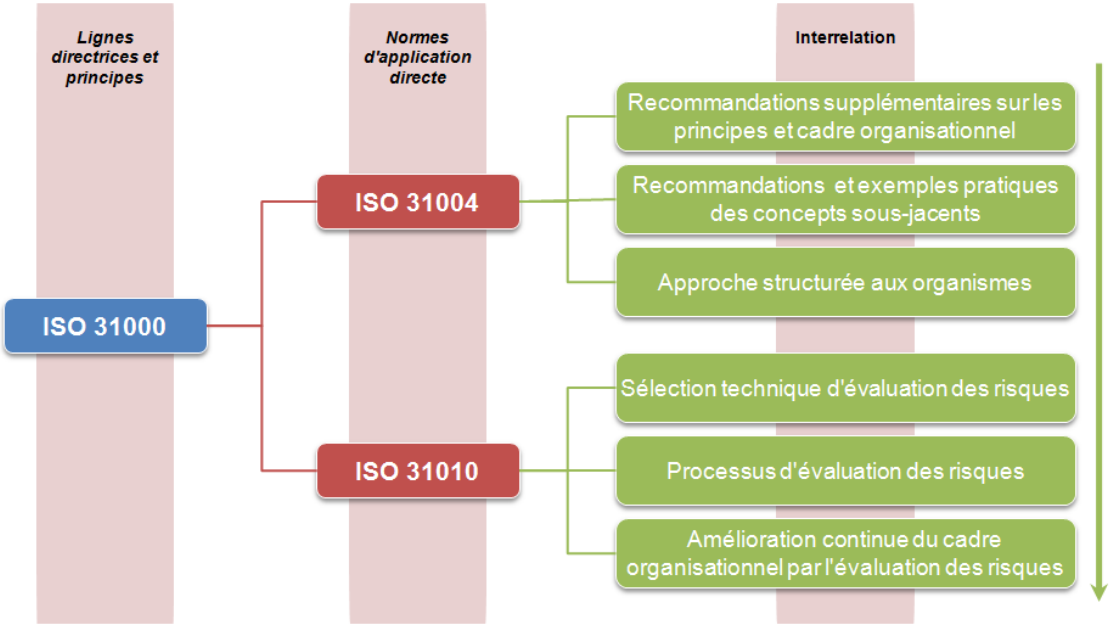


Figure 7 : Lien entre les normes ISO 31000, 31004 et 31010 *[source : auteurs]*

L'ISO 31000 propose le schéma ci-dessous qui permet de visualiser de façon plus détaillée, le lien entre les différentes normes du management du risque.

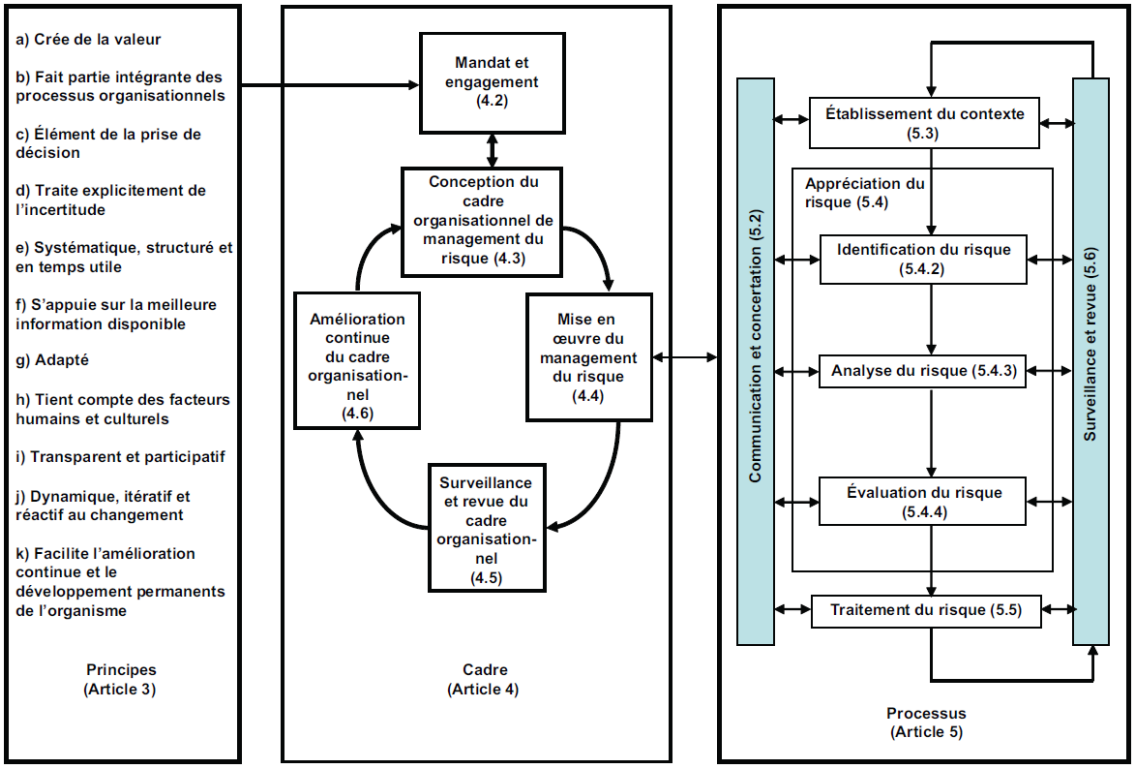


Figure 8 : Relation entre les principes, le cadre organisationnel et le processus du management du risque [7]

Cette figure met en exergue l'ensemble du processus définit par la norme ISO 31000 réalisable via les normes ISO 31004 et 31010 qui permettent l'établissement du contexte jusqu'à la surveillance.

## 2.2. Choix des outils

Pour répondre principalement aux besoins des TPE, PME et ETI, il semble judicieux d'utiliser deux outils qui auront l'avantage de laisser l'utilisateur libre de partir du point où il le souhaite dans sa recherche de compréhension du management du risque et ainsi débuter sa mise en œuvre du management du risque.

Pour ce faire, deux outils semblent pouvoir répondre à cette souplesse de mise en place du management du risque : l'interface web dynamique et l'autodiagnostic.

### 2.2.1. Interface web dynamique

| 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 9 : Choix du support pour l'interface web *[source : auteurs]***

Pour l'interface web, le SCENARIChain© [21] est l'outil qui est le plus ergonomique donc il sera facile d'utilisation et de compréhension. La seule lacune relevée concerne le manque de reconnaissance de cet outil. D'autres outils tels que Word® ou Excel® aurait pu être envisageable mais l'un des objectifs majeurs de la création d'outils de l'aide à l'implémentation de la norme ISO 31000 est sa praticité et son aspect convivial.

Une présentation sous SCENARIChain© va permettre de présenter sous forme d'une interface web dynamique la structure de la norme ISO 31000 avec :

- une première vue sur les trois articles de base : principe, cadre organisationnel, processus ;
- compléter par une deuxième vue présentant à son tour les sous tâches associées à chaque article ;
- puis un troisième niveau expliquant le contenu et les objectifs individuels de chaque sous tâche.

Cette approche permettra à la personne intéressée :

- de se déplacer librement dans l'arborescence ainsi créée ;
- d'avoir une lecture rapide du contenu de la norme.

### 2.2.2. Autodiagnostic

Pour l'Autodiagnostic, le choix du format Excel® semble le plus pertinent pour pouvoir répondre aux questions suivantes :

- ✓ Où doit s'appliquer le management du risque dans mes différents services ?
- ✓ Où en suis-je de ma gestion du management du risque ?
- ✓ Quels sont les points que dois-je améliorer ?

En effet, par le biais d'un questionnaire associé à une évaluation de la situation, ce type de programme est en mesure de générer des représentations graphiques des données recueillies sous forme de radar dans notre cas. Également, Excel® est outil relativement connu et utilisé par l'ensemble des organisations.

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

**Figure 10 : Choix du support pour l'outil autodiagnostic *[source : auteurs]***

Cette visualisation va ainsi permettre de :

- donner une lecture rapide à un temps $T^0$ de la situation,
- mettre en évidence les points présentant des faiblesses face à l'intégration des risques dans les processus et méthodes de travail,
- suivre à intervalle régulier les évolutions relatives au management du risque et donc à sa compréhension et son acceptation.

Le fichier sera bâti en partant de l'ISO 31000 pour la trame de base puis compléter à l'aide de l'ISO 31004 et 31010.

# 3. ABOUTISSEMENT DES OUITLS

## 3.1. L'interface web sous SCENARIChain©

Il va permettre de visualiser trois articles de la norme ISO 31000 à partir de fenêtre dynamique web. Le lecteur va ainsi se déplacer librement dans l'arborescence créé suivant ses besoins et attentes. Revenir en arrière ou passer à un autre article sans difficulté.

### 3.1.1. Structure de l'interface web

La page d'accueil de la norme permet d'accéder aux trois articles informant sur les points à suivre pour un management du risque intégré aux processus de l'organisme.

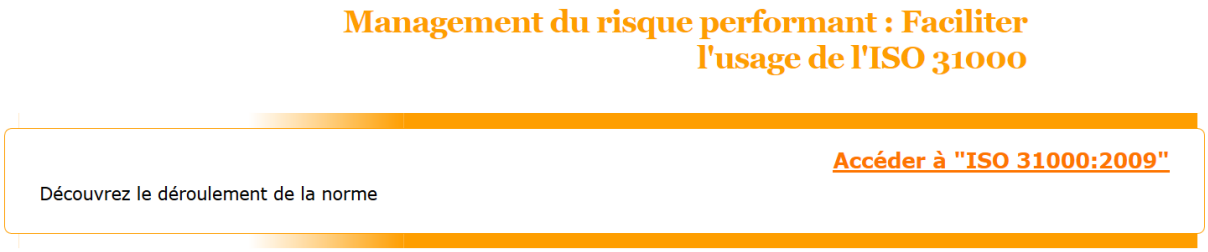


**Figure 11 : Page d'accueil web *[source : auteurs]***


**Figure 12 : Représentation graphiques des trois articles de la norme et son annexe *[source : auteurs]***

### 3.1.2. Mode d'utilisation de l'interface web

Des onglets actifs sont créés au niveau des représentations graphiques permettant d'atteindre le sous niveau correspondant.
Suivant les niveaux, diverses informations sont présenter dans les onglets comme :

- définitions (liées à la tâche visionnée)
- acteurs (pour la tâche visionnée)
- entrées / sorties (pour rendre opérationnelle la tâche présentée)
- outil (pouvant accompagner la réalisation de ce point de la norme)

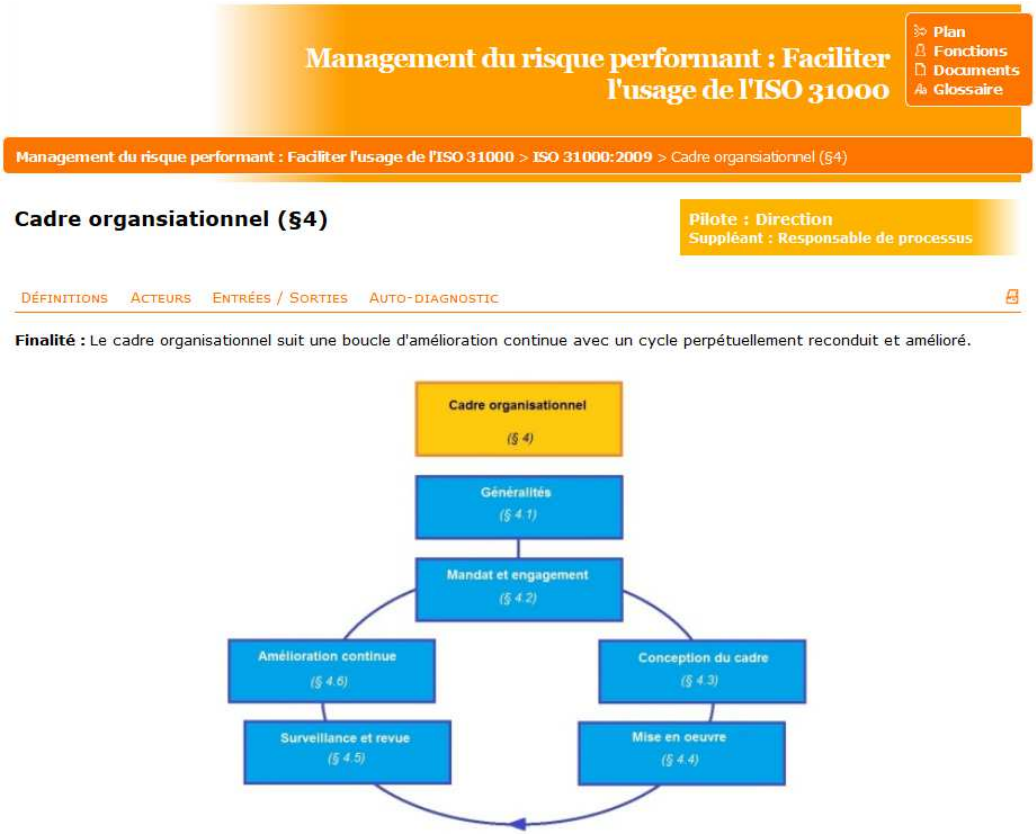


**Figure 13 : Représentation graphique de l'article 4 et onglets d'information**
***[source : auteurs]***

Dans le dernier niveau de l'arborescence, le développement du contenu d'un item avec les étapes à suivre, des remarques et des informations.

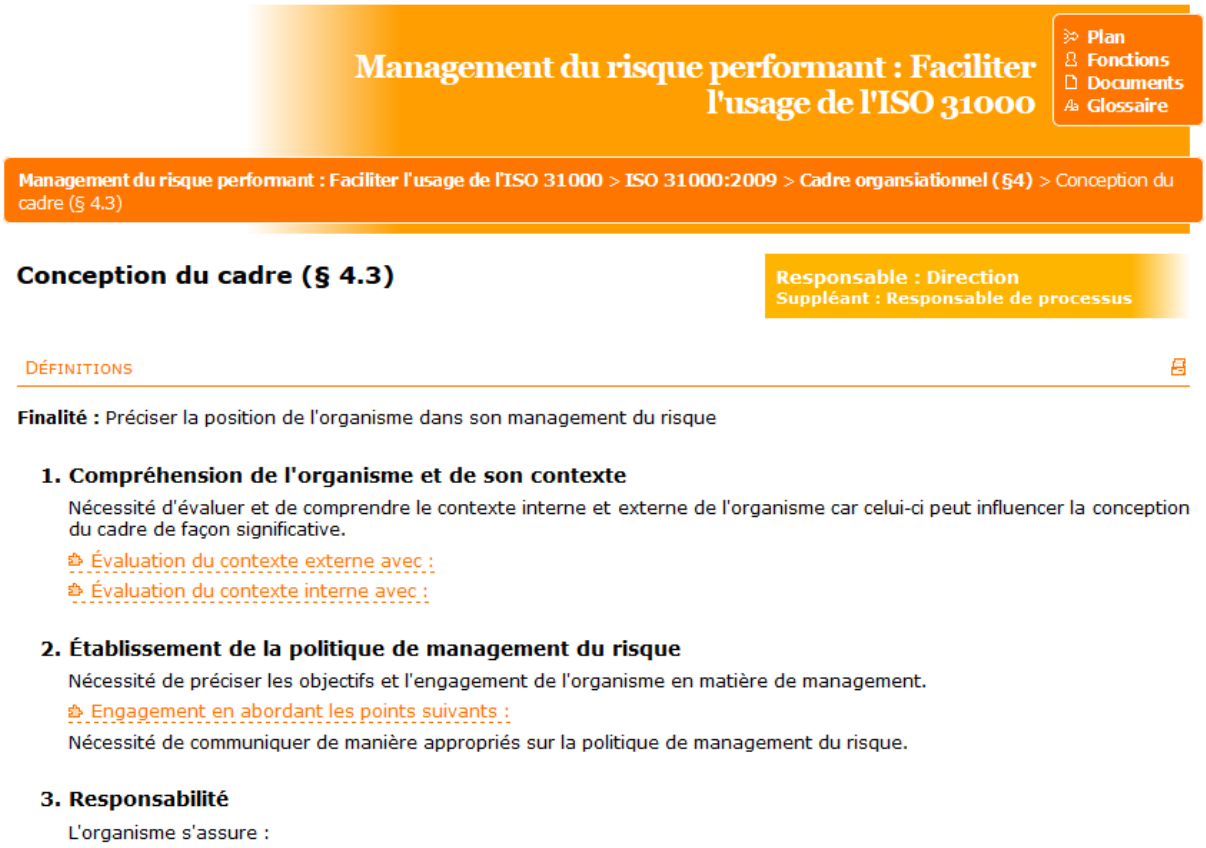


**Figure 14 : Extrait du dernier niveau de l'arborescence *[source : auteurs]***

Présent en haut à droite de chaque page, quatre items sont mis à disposition donnant accès au :

- Plan (visualisation de la trame des différentes fenêtres)
- Fonctions
- Documents
- Glossaire

## 3.2. Outil d'Autodiagnostic

### 3.2.1. Structure de l'outil d'Autodiagnostic

#### *3.2.1.1. Mode d'emploi*

Le mode d'emploi sert d'introduction à l'outil d'autodiagnostic, en expliquant en quoi consiste l'outil et comment l'utiliser. L'onglet « Mode d'emploi » se compose de quatre parties essentielles, comme le montre la figure ci-dessous.

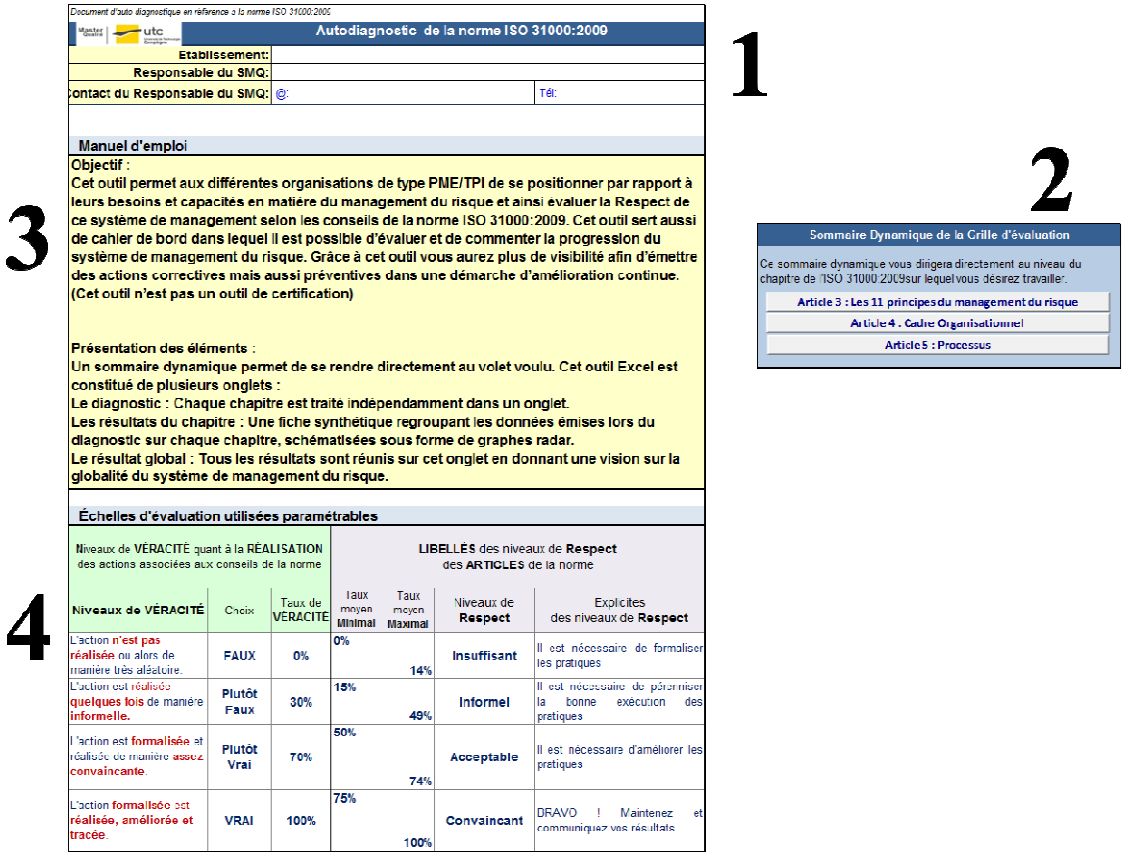


**Figure 15 : Onglet Mode d'emploi de l'outil autodiagnostic *[source : auteurs]***

1 → L'entête : permet d'identifier des informations concernant l'organisme et le responsable SMQ.

2 → Sommaire dynamique : permet une navigation rapide entre les différents articles traités dans l'outil d'autodiagnostic.

3 → Le manuel d'emploi : définit les objectifs de l'outil d'autodiagnostic ainsi qu'une brève présentation des éléments dont il se compose.

4 → Échelles d'évaluation : définit les niveaux de véracité sur lesquels est basé l'outil d'autodiagnostic ainsi que les taux et les niveaux de conformités auxquels ils sont associés.

### 3.2.1.2. La grille d'évaluation

La grille d'évaluation est constituée de critères à évaluer, ces critères sont des recommandations tirés des différents articles de la norme ISO 31000:2009. Ils sont exprimés sous forme de phrase affirmative et sont arrangés par article et sous article. Par critère, l'évaluateur choisit un niveau de véracité qui va générer automatiquement un taux.

L'onglet comportant les grilles d'évaluation inclut des boutons de navigation permettant d'accéder aux différents articles de l'outil ainsi qu'aux résultats des articles.

La figure ci-dessous représente un aperçu de l'onglet de grille d'évaluation.

*Document d'autodiagnostic en référence à la norme ISO 31000:2009*

| Autodiagnostic sur l'Article 5: Processus | | | | | |
|---|---|---|---|---|---|
| **Etablissement:** | | - | | | |
| **Date** de l'autodiagnostic (jj/mm/aaaa) : | | | | | Signature de l'évaluateur : |
| **Responsable** de l'évaluation : | | | | | |
| **L'équipe** d'évaluation: | | | | | |
| **Contact** de la responsable : | | Tél: | | @ | |
| | | | | | |
| **Réf.** | **Items des articles de la norme** | **Evaluations** | **Taux %** | **Libellés des évaluations** | **Modes de preuve et commentaires** |
| **Art .5** | **Processus** | **Convaincant** | **77%** | **BRAVO ! Maintenez et communiquez vos résultats** | |
| **5.1** | **Généralités** | **Informel** | **43%** | **Il est nécessaire de pérenniser la bonne exécution des pratiques** | |
| 1 | Le management du risque est une partie intégrante du management. | Plutôt Faux | 30% | L'action est réalisée quelques fois de manière informelle. | |
| 2 | Le management du risque est intégré à la culture et aux pratiques. | Choix / FAUX / Plutôt Faux / Plutôt Vrai / VRAI | 30% | L'action est réalisée quelques fois de manière informelle. | |
| 3 | Le management du risque est adapté aux processus métiers de l'organisme. | Plutôt Vrai | 70% | L'action est formalisée et réalisée de manière assez convaincante. | |

**Figure 16 : Extrait de la grille d'évaluation de l'outil autodiagnostic *[source : auteurs]***

### 3.2.1.3. La feuille de synthèse des résultats et les représentations graphiques pour chaque article

L'onglet résultat est constitué de schémas donnant une représentation graphique simple et communicative du niveau de satisfaction de chaque article traité. A l'issue de l'évaluation de chaque article de la norme, l'utilisateur peut noter ses remarques et ses plans d'actions dans l'onglet des résultats.

L'outil d'autodiagnostic permet de visualiser les résultats de chaque article séparément. Le fait d'avoir une évaluation détaillée de chaque article de la norme va permettre aux utilisateurs d'avoir une visibilité optimale sur les lacunes à améliorer. La figure ci-dessous donne un aperçu sur l'onglet de résultat.

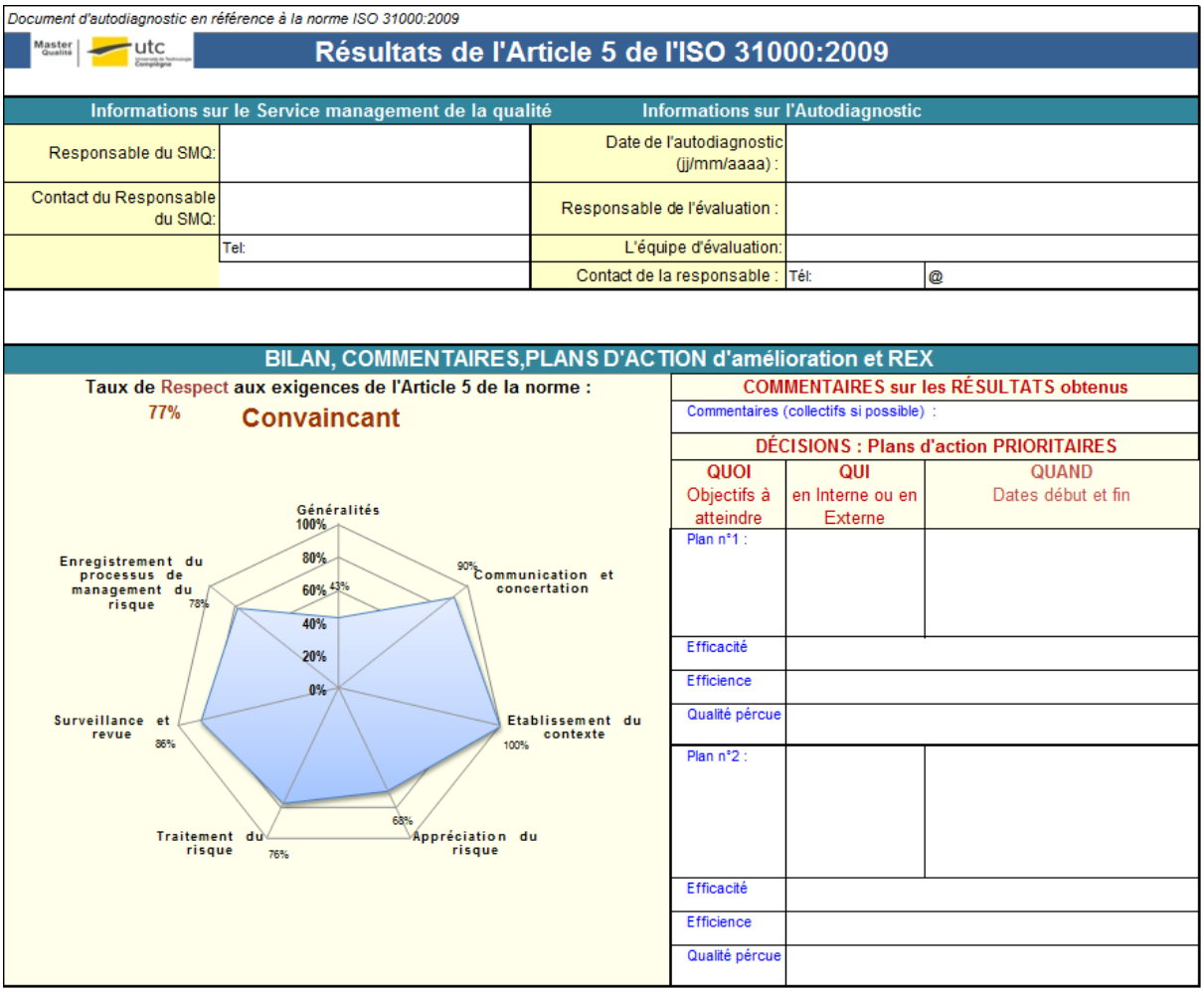


**Figure 17 : Aperçu de l'onglet résultat de l'outil autodiagnostic *[source : auteurs]***

### *3.2.1.4. La feuille de synthèse des résultats et les représentations graphiques générales*

L'outil d'autodiagnostic permet de synthétiser les différents niveaux de satisfaction de l'ensemble des articles de la norme par des représentations graphiques. Cette représentation graphique permet aux utilisateurs de prioriser les actions correctives et préventives et par conséquent mettre en place un plan d'action traitant les points sensibles et critiques recensés à l'issu de l'évaluation. Pour ce faire, un tableau a été mis en place afin de réunir l'ensemble des remarques, notes et plans d'actions proposés. La figure ci-dessous donne un aperçu sur l'onglet de résultat global.

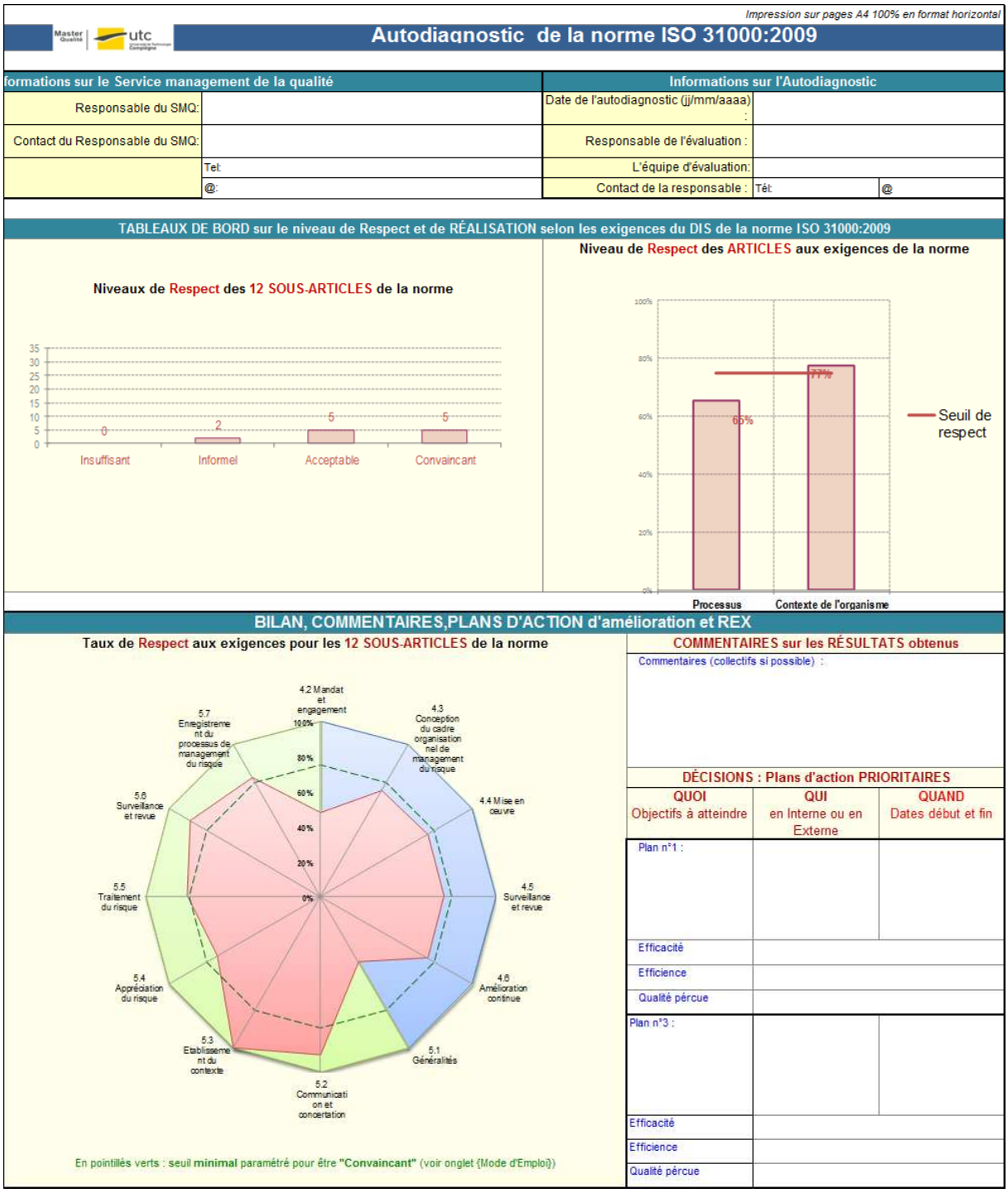


**Figure 18 : Aperçu de l'onglet résultat global *[source : auteurs]***

### 3.2.2. Processus de l'utilisation de l'outil d'Autodiagnostic

Le logigramme suivant détaille la démarche optimale à suivre afin d'obtenir un résultat d'évaluation conforme à l'aide de l'outil d'autodiagnostic.

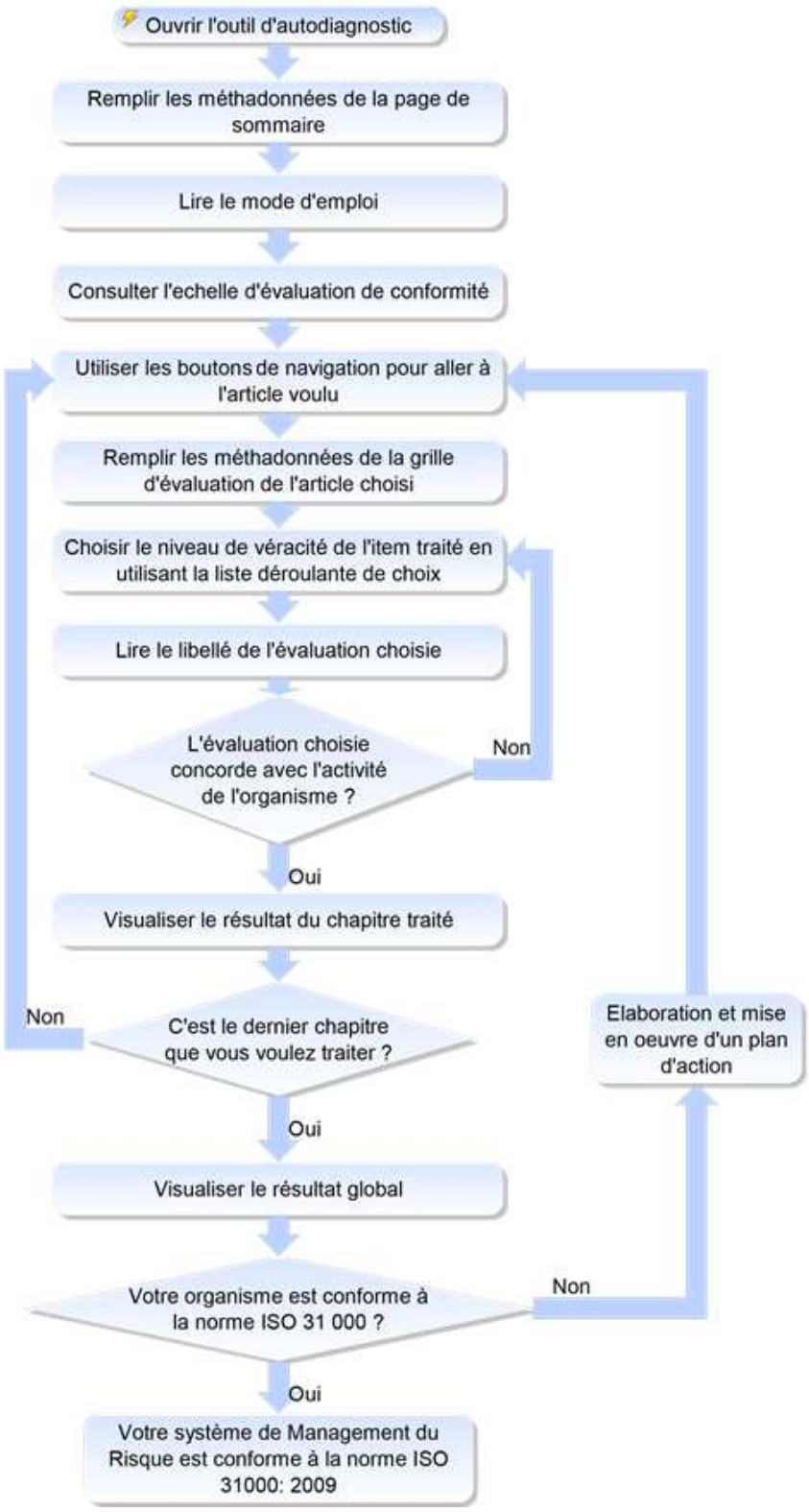


**Figure 19 : Logigramme d'utilisation de l'outil d'autodiagnostic *[source : auteurs]***

## 3.3. Bilan

Les outils mis en place sont adaptables à tout type d'organisme et libre d'accès offrant ainsi à chacun la possibilité de les faire évoluer en fonction de ses besoins, de sa structure et de son activité. Ils sont simples d'utilisation et offrent une manipulation plus aisée et intuitive que d'autres supports. Ils permettent d'appréhender de manière interactive le contenu de la norme ISO 31000, 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 améliorant ainsi durablement la performance.

# Conclusion

La gestion du risque est une notion relativement récente dans les organismes. Afin de bien comprendre son évolution, il est indispensable de disposer de certains repères historiques. Au début la gestion du risque s'apparentait à un simple renvoie vers les assurances. Au fil des années, la gestion du risque a évolué avec notamment la notion de « cartographie des risques ». Il s'agit d'identifier les risques, de les évaluer et d'élaborer des moyens de contrôles et de maîtrises. La gestion du risque apparaît comme un enjeu primordial pour les organismes. C'est un outil de pilotage opérationnel et d'aide à la décision stratégique qui nécessite l'engagement des plus hautes instances de l'organisme, une communication soutenue entre les différentes parties ainsi qu'un travail de mise à jour permanent.

Avec la mondialisation et la complexification des activités et les réglementations, l'organisme doit faire face à l'émergence des risques de plus en plus nombreux et diversifiés. De ce fait, le risque n'est plus un critère étudié et géré séparément du reste des processus. Il est à unifier avec tous les processus pour être amené à faire face à un monde complexe, instable et incertain. Maîtriser les risques, réduire les menaces et saisir les opportunités, c'est concourir au développement de l'entreprise, au profit de toutes ses parties prenantes. Intégré au pilotage de l'organisation, le management du risque est un remarquable outil d'efficience qui facilite la prise de décision et l'atteinte des objectifs [22].

L'objectif de ce projet « Management du Risque Performant : faciliter l'usage de l'ISO 31000 » est d'aider les organismes (surtout type TPE, PME et ETI) à implémenter le management du risque liés aux activités effectuées et à l'intégrer dans leur système managérial. En se référant aux recommandations de la norme ISO 31000 version 2009, qui fournit des principes et des lignes directrices, et en se basant sur les difficultés rencontrées par les organismes en matière de gestion du risque, deux outils simples et conviviaux ont été élaborés.

Dans un premier temps, une interface web basée sur SCENARIChain© a été élaborée. Il s'agit d'un outil simple et interactif, qui permet, à la fois, à l'utilisateur de se déplacer librement dans l'arborescence et d'avoir une lecture rapide du contenu de la norme ISO 31000:2009.

Dans un second temps, un outil d'autodiagnostic sous format Excel®, bâti sur les deux principaux articles de cette dernière norme et complété à l'aide de l'ISO 31004 et 31010. Cet outil, par le biais d'un questionnaire associé à une évaluation de la situation, permet de donner une idée sur la situation actuelle de l'organisme et par la suite de mieux se connaître en matière de gestion de risque. Il génère des représentations graphiques des données recueillies. A des intervalles réguliers, l'organisme peut refaire le test pour suivre son évolution.

Pour finir et pour aller plus loin, il est à souligner que des recherches effectuées ont montré que l'intégration des risques dans tous les processus et cela dès leurs créations ou au cours de leurs mises à jours suite aux revues réalisées par les organismes devient de

plus en plus prégnant dans les discours et dans les évolutions des méthodes de management.

Ainsi, en France, la commission de normalisation Management des risques (AFNOR/CN Risque) [23], [24] travaille sur des documents complémentaires qui verront le jour suivant le programme ci-après :

| Référence | Titre | Motif de la filière d'origine | Publication |
|---|---|---|---|
| PR FD X50-260 | Management des risques<br>Lignes directrices pour la mise en œuvre dans les ETI / PME | Nouveau document | Janvier 2016 |
| ISO 31000 | Management du risque<br>Principes et lignes directrices | Révision du document | Août 2017 |
| ISO GUIDE 73 | Management du risque<br>Vocabulaire | Révision du document | Août 2017 |
| ISO/NP 31020 | Management du risque lié à l'interruption d'activité | Nouveau document | Octobre 2017 |
| ISO/AWI 31021 | Management du risque de la chaîne d'approvisionnement<br>Une compilation des meilleurs pratiques | Nouveau document | Novembre 2017 |
| ISO 20812 | Guidelines for implementation of entreprise legal risk management | Nouveau document | Juillet 2018 |

**Figure 20 : Documents normatifs à paraître et relatif au management du risque [23]**

La norme ISO 31000 n'est pas encore une norme d'exigence. La deviendra-t-elle ? A priori, les obligations légales, les interprétations d'un même risque n'ayant pas la même valeur d'un organisme à l'autre, d'un pays à l'autre, cela ne semble pas envisageable dans le contexte actuel [22].

L'ISO 9001:2015 ayant intégré le traitement du risque dans ses exigences [25], où en serait l'intérêt ?

# Bibliographie

[1] INSEE, « Définitions, méthodes et qualité, Définitions ». INSEE, www.insee.fr.

[2] J.-F. PILLOU, « Le bug de l'an 2000 ». CCM, www.comentcamarche.net, sept-2015.

[3] Institut National de l'Audiovisuel, « Attentats Etats-Unis : le film de la catastrophe », *www.ina.fr*. [En ligne]. Disponible sur: http://www.ina.fr/video/1820710002004. [Consulté le: 28-janv-2016].

[4] 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.

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

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

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

[8] 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.

[9] G. MOTET, *La norme ISO 31000 en 10 questions*. France: Institut pour une Culture de Sécurité Industrielle, 2009.

[10] « Définition : Enjeu ». LAROUSSE, www.larousse.fr.

[11] 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.

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

[13] FERMA, « FERMA European Risk Management Benchmarking Survey 2012 », Ed. FERMA, benchmarking-survey-2012-presentation.pdf, oct. 2012.

[14] AFNOR, « NF EN ISO 9001 Systèmes de management de la qualité — Exigences ». Edition Afnor, www.afnor.org, oct-2015.

[15] AFNOR, « NF EN ISO 14001 Systèmes de management environnemental — Exigences et lignes directrices pour son utilisation ». Edition Afnor, www.afnor.org, oct-2015.

[16] AFNOR, « NF EN ISO 13485 Dispositifs médicaux _ Systèmes de management de la qualité _ Exigences à des fins réglementaires ». Edition Afnor, www.afnor.org, sept-2012.

[17] AFNOR, « NF ISO 26000 Lignes directrices relatives à la responsabilité sociétale ». AFNOR, www.afnor.org, nov-2010.

[18] AFNOR, « FD ISO 31004 Lignes directrices pour l'implémentation de l'ISO 31000 ». Edition Afnor, www.afnor.org, 14-oct-2015.

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

[20] « ISO Focus+, Février 2013 - ISO », *ISO Focus*+, vol. 4, n° 2, p. 33, févr-2013.

[21] UTC et KELIS, « SCENARIChain 4.1 ». Ed. KELIS, www.scenari-platform.org, nov-2015.

[22] J. LE RAY, *De la gestion des risques au management des risques. Pourquoi ? Comment ?* AFNOR Editions, www.afnor.org, 2015.

[23] R. CIVET, « Commission normalisation Management des risque : AFNOR/CN Risque », *www2.afnor.org/espace_normalisation*. [En ligne]. Disponible sur: http://www2.afnor.org/espace_normalisation/structure.aspx?commid=55774#retour. [Consulté le: 09-nov-2015].

[24] S. TRANCHARD, « The revision of ISO 31000 on risk management has started ». ISO, www.iso.org, mai-2015.

[25] M. LAZARTE, « ISO 9001:2015 - Just published! » ISO, www.iso.org, sept-2015.

[26] *Code du travail - Article L4121-2*, vol. L4121□2. .

# Lexique

**Analyse du risque :** processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque. Elle fournit la base de l'évaluation du risque et les décisions relatives au traitement du risque et inclut l'estimation du risque.

**Appréciation du risque :** processus de recherche, de reconnaissance et de description des risques.

**Attitude face au risque :** approche d'un organisme pour apprécier un risque avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque.

**Autodiagnostic :** est une analyse de l'ensemble des composantes d'un élèment afin d'en ressortir ses forces et ses faiblesses.

**Benchmarking :** est un processus d'analyse de la concurrence, dont le but principal est de pouvoir augmenter la performance de l'entreprise.

**Cadre organisationnel de management du risque :** ensemble d'éléments établissant les fondements et les dispositions organisationnelles présidant la conception, la mise en œuvre, la surveillance, la revue et l'amélioration continue du management du risque dans tout l'organisme.

**Communication et concertation :** processus itératifs et continus mis en œuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les parties prenantes et autres parties, concernant le management du risque.

**Conséquence :** effet d'un événement affectant les objectifs.

**Contexte externe :** environnement externe dans lequel l'organisme cherche à atteindre ses objectifs.

**Contexte interne :** environnement interne dans lequel l'organisme cherche à atteindre ses objectifs.

**Établissement du contexte :** définition des paramètres externes et internes à prendre en compte lors du management du risque et définition du domaine d'application ainsi que des critères de risque pour la politique de management du risque.

**Évaluation du risque :** processus de comparaison des résultats de l'analyse du risque avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables.

**Événement :** occurrence ou changement d'un ensemble particulier de circonstances.

**Logigramme :** décrit de façon détaillée un processus, en le découpant en étapes.

**Management du risque :** activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du risque.

**Moyen de maîtrise :** mesure qui modifie un risque.

**Niveau de risque :** importance d'un risque ou combinaison de risques, exprimée en termes de combinaison des conséquences et de leur vraisemblance.

**Partie prenante :** personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité.

**Plan de management du risque :** programme inclus dans le cadre organisationnel de management du risque, spécifiant l'approche, les composantes du management et les ressources auxquelles doit avoir recours le management du risque.

**Politique de management du risque :** déclaration des intentions et des orientations générales d'un organisme en relation avec le management du risque.

**Processus de management du risque :** application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques.

**Processus :** est un ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie.

**Profil de risque :** description d'un ensemble quelconque de risques.

**Propriétaire du risque :** personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer.

**Revue :** activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis.

**Risk Management :** est l'identification, l'évaluation et la hiérarchisation des risques

**Risque résiduel :** risque subsistant après le traitement du risque.

**Risque :** effet de l'incertitude sur l'atteinte des objectifs.

**ScenariChain© :** est une chaîne éditoriale développée au sein de l'IUT de Compiègne. Elle permet de créer des supports de cours diffusables sous forme de fichier texte (format Open Document Texte), de site web (dossier de pages html) ou de diaporama (dossier de pages html).

**Source de risque :** tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un risque.

**Surveillance :** vérification, supervision, observation critique ou détermination de l'état afin d'identifier continuellement des changements par rapport au niveau de performance exigé ou attendu.

**Traitement du risque :** processus destiné à modifier un risque.

**Vraisemblance :** possibilité que quelque chose se produise.

# Annexes

ANNEXE A – Les différentes catégories de risque

ANNEXE B – Planification dynamique stratégique

# ANNEXE A – Les différentes catégories de risque

Dans ces ouvrages [11], [12] Jean-David DARSA classe les risques en 11 catégories.

### *Risques géopolitiques*

Ce sont les risques liés à l'environnement global de l'organisme hors de ses frontières. Quand une organisation évolue à l'extérieur de son pays d'origine, elle devient exposée au « risque pays » où sont localisées ses activités.

Blocus économique, attentats, guerres, climat insurrectionnel, catastrophes naturelles, mouvements sociaux, instabilité économique, politique ou social, tels sont les risques majeurs à appréhender et à traiter, pays par pays, zones géographiques par zones géographiques.

### *Risques économiques*

Les risques économiques regroupent l'ensemble des risques associés à l'activité économique des organismes. Inflation, évolution de la demande, des besoins, des marchés, des conditions de financement, l'évolution de la disponibilité et de la rareté des ressources financières … sont tous des risques susceptibles de remettre en cause ou de déstabiliser la structure de la chaîne de valeur de l'organisme.

### *Risques stratégiques*

Une organisation, quelle que soit sa taille, propose un modèle stratégique pour atteindre ses objectifs. L'incohérence entre les différents segments constitutifs du modèle stratégique est une source de risques. La constitution, la validité, la robustesse, la capacité d'ajustement et de réponse des processus cibles composant le modèle stratégique seront le cœur de la réussite de tout organisme.

### *Risques financiers*

La mise en œuvre du modèle stratégique engendre la création d'une multitude de risques financiers. Du risque d'illiquidité au risque de taux de change, du risque de crédit au risque de dilution du capital, du risque de financement aux risques comptables et fiscaux …

Tout risque, toute classe de risques, toute décision d'organisme autre aura une incidence financière sur l'organisme, donc favorisera l'émergence potentielle d'un risque financier.

### *Risques opérationnels*

Les risques opérationnels matérialiseront tous les impacts directs ou indirects engendrés par l'organisme dans son activité quotidienne, dans son cycle d'exploitation (infrastructures, énergies, cycles de production, de distribution, d'approvisionnement, processus logistique, gestion documentaire, …).

### *Risques industriels*

Les risques industriels couvrent une catégorie particulière de risques opérationnels, rencontrés exclusivement dans les activités de fabrication, de transformation, donc de production de biens.

### Risques juridiques

Ils couvrent les problématiques contractuelles des relations d'affaires, des obligations de respect de la conformité des lois et des règles en vigueur (notion de conformité juridique), les problématiques liés à la contrefaçon, ainsi que la responsabilité pénale du dirigeant.

Il est important de maintenir une vigilance aux risques juridiques auxquels est exposé l'organisme car ils constituent un véritable piège pour les organismes à court, moyen et long terme. Aujourd'hui, la pénalisation du monde des affaires est croissant et le nombre de textes et de décrets réglementaires se multiple rendant la connaissance illisible.

### Risques informatiques

Les risques informatiques sont une source permanente de risques critiques pour les organismes de nos jours, compte tenu de l'usage intensif des outils informatiques (matériels, logiciels, applications, infrastructures réseaux, …). Quelle que soit la taille de l'organisation, l'outil informatique est essentiel à l'activité quotidienne, et la pérennité de l'infrastructure informatique devient indispensable. Afin de pouvoir se défaire de ce risque ou le limiter, la norme ISO 27000 fournit une vue d'ensemble des systèmes de management de la sécurité de l'information.

### Risques sociaux et psychosociaux

Les risques sociaux (climat social, maîtrise du turn-over, gestion de la compétence, perte homme clé, …) et les risques psychosociaux (mal-être, stress, harcèlement sexuel et/ou moral, suicide, conduites additives, …) sont tout aussi présents. Cette classe de risques, nécessitera un traitement particulier et primordial. Dans le droit positif, l'article L.4121-1 du Code du travail [26] illustre l'ensemble des risques psychosociaux que peuvent rencontrer les salariés. L'employeur se fonde sur les principes généraux de prévention afin de combattre les risques à la source et d'adapter le travail à l'homme. Il faut intervenir le plus en amont possible pour prévenir les risques psychosociaux.

### Risques d'image ou de réputation

L'image qu'affiche un organisme auprès de ses salariés, de ses clients, de ses fournisseurs, de ses partenaires, de ses tiers de confiance est très importante. Sa destruction ou sa dégradation constitue des risques indéniables dont les impacts en termes de gravité seront très lourds, voire impossibles à surmonter (contrefaçon, rumeurs, concurrence déloyale, espionnage industriel, …).

### Risques de knowledge management

La connaissance et les savoir-faire de l'organisation, son évolution et sa capitalisation exposent tous les organismes aux risques liés au « knowledge management », autrement dit à la gestion de la connaissance. La maîtrise de ces risques permet d'optimiser l'efficacité de l'activité.

# ANNEXE B – Planification dynamique stratégique