



La boîte à outils pour le management du risque

par Maria Lazarte et Sandrine Tranchard

Les organismes ou entreprises peuvent dès à présent bénéficier d'une boîte à outils complète pour le management du risque comprenant :

- ISO 31000:2009, *Management du risque – Principes et lignes directrices*
- Guide ISO 73:2009, *Management du risque – Vocabulaire*
- ISO/CEI 31010:2009, *Gestion des risques – Techniques d'évaluation des risques.*

Faire face aux incertitudes

Les risques auxquels sont confrontés les organismes ou entreprises peuvent avoir des conséquences en termes de résultats sociétaux, environnementaux, technologiques, de sécurité et de sûreté, de mesures commerciales, financières et économiques, et avoir des impacts sociaux, culturels, sans oublier qu'ils peuvent toucher à la réputation politique. ISO 31000:2009 aidera les organismes de tous types et de toutes dimensions à gérer efficacement les risques.

ISO 31000 fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque d'une manière transparente, systématique et crédible dans quelque domaine et quelque contexte que ce soit. Elle recommande aux organismes d'élaborer et de mettre en œuvre un cadre de management du risque, qui sera intégré à leur système de management général et constamment amélioré.

Pour Kevin W. Knight, AM ¹⁾, Président du groupe de travail ISO qui a élaboré la norme, «ISO 31000 est un document concret qui vise à aider les organismes à développer leur propre approche du management du risque, mais ce n'est pas une norme applicable à une démarche de certification. En mettant en œuvre ISO 31000, ils peuvent évaluer leurs pratiques en matière de management du risque en fonction d'un référentiel reconnu au niveau international, offrant des principes rigoureux pour un management efficace.»

Le Guide ISO 73:2009, *Management du risque – Vocabulaire*, complète ISO 31000 en fournissant un ensemble de termes et définitions relatifs au management du risque.

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

1) Membre de l'Ordre d'Australie

- 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 opérationnelles,
- 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.

Pour M. Knight, « le risque est inhérent à toute activité. On peut même alléguer que la crise financière mondiale résulte d'une mauvaise gestion du risque par les conseils d'administration et les équipes de direction. ISO 31000 devrait aider l'industrie et le commerce, le public et le privé, à sortir de la crise sur de nouvelles bases de confiance. »

L'évaluation du risque

Quand des risques se présentent, les organismes doivent toujours se demander: «Le niveau de risque est-il tolérable ou acceptable? Nécessite-t-il un traitement plus en profondeur?»

L'évaluation du risque fait partie intégrante du management du risque; elle consiste à fournir un processus structuré permettant aux organismes d'évaluer dans quelle mesure leurs objectifs peuvent être affectés, d'analyser les conséquences ainsi que la vraisemblance de celles-ci et la probabilité d'occurrence des risques avant de décider s'il est nécessaire de procéder à un traitement supplémentaire.

La troisième norme, ISO/CEI 31010:2009, *Gestion des risques – Techniques d'évaluation des risques*, a été élaborée conjointement par l'ISO et la CEI (Commission électrotechnique internationale).

L'évaluation du risque donne aux décideurs et aux parties responsables une meilleure compréhension des risques pouvant gêner la réalisation des objectifs et leur



permet d'évaluer l'adéquation et l'efficacité des contrôles déjà mis en place. La norme fournit une base sur laquelle s'appuyer pour décider de la meilleure manière de traiter des risques particuliers et de faire un choix parmi différentes options.

ISO/CEI 31010 aidera les organismes à mettre en oeuvre les principes et lignes directrices relatifs au management du risque de la norme ISO 31000.

La norme ISO/CEI 31010 reflète les bons usages actuels et répond aux questions suivantes:

- 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 ?

L'application de certaines techniques est présentée, avec des références spécifiques à d'autres Normes internationales. L'évaluation du risque n'est pas une activité autonome. Il convient qu'elle soit totalement intégrée aux autres composantes du processus de management des risques.

Pour Eric Mahy, Chef de projet pour cette norme, «ISO/CEI 31010 s'adresse aux novices du management du risque comme aux professionnels du risque les plus avertis. Elle s'intègre à un ensemble structuré de

normes relatives au management du risque, qui a été développé dans l'optique de proposer une approche «meilleure pratique».

Une boîte à outils pour tous

La norme ISO 31000, le Guide ISO 73 et l'ISO CEI 31010 peuvent être appliqués par toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu et sont utiles notamment pour :

- Les personnes chargées du management du risque dans leur organisation
- Les personnes chargées de s'assurer que ce risque est géré efficacement
- Les personnes chargées d'évaluer les pratiques d'un organisme en matière de management du risque
- Les rédacteurs de normes, guides, procédures et bonnes pratiques en matière de management des risques.

ISO 31000 et le Guide ISO 73 ont été préparés par le groupe de travail ISO sur le management du risque. ISO/CEI 31010:2009 a été préparée conjointement par le comité d'études 56 de la CEI, *Sûreté de fonctionnement*, et le groupe de travail ISO sur le management du risque.

Maria Lazarte Rédactrice adjointe, ISO Focus+.
Sandrine Tranchard, Chargée de communication,
Secrétariat central de l'ISO.

