
DR

Réaction de Alex Dali, *directeur associé d'Atlascope**

Les enjeux de **la norme ISO 31000** en gestion des risques

La future norme ISO 31000 (management des risques, principes et lignes directrices de mise en œuvre) est en cours de finalisation et devrait s'imposer comme le cadre de référence international en gestion des risques.

Récemment finalisée, la norme ISO 31000 (lire encadré ci-dessous) a été rédigée pour l'essentiel à partir de la norme australienne AS/NZS 4360. Elle définit les lignes directrices du management des risques et les processus de mise en œuvre au niveau stratégique et opérationnel.

STRUCTURE DE LA NORME ISO 31000

La norme est structurée en trois parties : les principes, le cadre organisationnel et le processus de management :

- Les principes répondent à la question « pourquoi fait-on du management des risques ? ». Le processus d'intégration de ces principes se fait ensuite à deux niveaux : décisionnel et opérationnel.
- Le cadre organisationnel explique comment intégrer, via le processus itératif de la roue de Deming (Plan-Do-Check-Act), le management des risques dans la stratégie de l'organisation (conduite stratégique).
- Le processus de management précise comment intégrer le management des risques au niveau opérationnel de la stratégie de l'organisation (conduite opérationnelle). Ce processus itératif est bien connu des risk managers (voir infographie). Il ne s'agit en aucun cas d'uniformiser les pratiques, ni de créer un système de management parallèle, comme certains l'ont pensé, à tort, de la norme ISO 9000. En revanche, la norme ISO 31000 propose un référentiel unique pour les organisations de tout secteur et de toute taille. Elle est adaptable et suffisamment flexible pour harmoniser les processus de management de tous les types de risques faisant peser une incertitude sur l'atteinte des objectifs de l'entreprise.

NOUVELLE DÉFINITION DU RISQUE

Le mot risque désigne une non-conformité en qualité, une pollution en environnement, une défaillance d'un équipement, une intoxication ou des atteintes corporelles en matière de sécurité des personnes, mais aussi un rendement en finance ou des opportunités pour le manager d'entreprise. La norme ISO 31000 visant à devenir le référentiel unique en matière de management des risques, une révision du guide ISO 73 – vocabulaire du management du risque – a été menée parallèlement aux développements de l'ISO 31000 afin de faciliter les discussions entre professionnels des risques (tous secteurs confondus). La nouvelle définition abandonne la vision de l'ingénieur (« le risque est la combinaison de probabilité d'événement et de sa conséquence ») pour coupler les risques aux objectifs de l'organisation : le risque est l'effet de l'incertitude sur l'atteinte des objectifs. Cette définition est extraite de la dernière version du guide ISO 73 qui sera publiée en même temps que la norme ISO 31000.

PAS DE CERTIFICATION

Le texte actuel de l'ISO 31000 est très clair : « *La présente norme internationale n'a pas vocation à servir de base à une certification.* » Cependant, certains pays seraient être ouverts à un tel processus à partir de la norme internationale. La norme BSI 31100 en Angleterre et l'ONR 49000 en Autriche (utilisé également en Allemagne et en Suisse) semblent s'orienter vers un tel processus. La norme AS/NZS4360 mise à jour en 2009 restera une obligation en Australie/Nouvelle-Zélande. Ces trois référentiels reprendront intégralement la norme ISO 31000. En France, l'Afnor, l'association française de normalisation, a participé activement aux débats au sein du comité ISO pour le management des risques et était représenté, en autres, par Jean-Paul Louisot, directeur pédagogique du Carm Institute, institut pour la formation ARM en France, et par Gilles Motet, directeur scientifique de l'ICSI, institut

La norme ISO 31000

– Historique :

- Juin 2004 : demande de reprise « fast-track » de l'AS/NZS 4360 refusée.
- Juin 2005 : lancement de la procédure ISO.
- Septembre 2005 : ISO 31000 sera un *guideline* non certifiable.
- Plusieurs réunions en 2006 et 2007.
- Avril 2008 : rédaction du Draft DIS et enquête.
- Début 2009 : vote des membres.
- Juin 2009 : publication probable.

– Points importants :

- Principes généraux et lignes directrices de mise en œuvre.
- Processus de management des risques orienté par rapport aux objectifs de l'organisation.
- Nouvelle définition du vocabulaire : risque = incertitude sur les objectifs.
- Impact négatif des risques (menaces) ou impact positif (opportunités).
- Importance de la communication à chaque étape.
- Toujours préciser le contexte interne et externe.
- Norme ISO non certifiable.

Globalement, la norme souligne que le management des risques fait partie intégrante de la structure, des responsabilités et des objectifs d'une organisation.

pour la culture et la sécurité industrielle. A ce jour, la plupart des associations nationales de gestion des risques (Amrae, Airmic, Belrim, etc.) ainsi que Ferma, la fédération européenne, sont opposées à la certification de cette norme.

PROBLÉMATIQUES DE LA NORME

Cependant, plusieurs éléments du standard sont à l'origine de vifs débats entre les représentants des associations nationales de normalisation. Par exemple, le fait que le standard se focalise sur la communication et la consultation, donc sur la perception des risques par les parties prenantes, a troublé plusieurs groupes nationaux, rapporte Kevin Knight, coordinateur du groupe de travail ISO 31000 et concepteur du standard australien de référence, créé il y a plus de dix ans.

Un autre sujet à controverse est la notion de risque « positif », qui a soulevé une opposition des responsables de santé, et plus encore des spécialistes d'hygiène/sécurité présents. « *Le consensus adopté est de parler de risque à conséquences positives (opportunités) ou négatives (menaces), car en matière d'hygiène/sécurité, le risque est intrinsèquement négatif, tandis qu'en matière de santé, il s'agit d'une stratégie thérapeutique arrêtée avec le patient et/ou sa famille* », explique Jean-Paul Louisot.

Autre difficulté : le besoin d'identifier, pour chaque risque, une seule personne comme « propriétaire du risque » (*risk owner*, en anglais) et, donc, comme seul responsable du management de ces risques. Les notions de responsabilité collective ou de « responsable, mais pas coupable » n'ont pas été accueillies favorablement par les instances du groupe ISO.

> Les notions de responsabilité collective ou de « responsable, mais pas coupable » **n'ont pas été accueillies favorablement** par les instances du groupe ISO.

« *Il faut souligner que dans l'esprit de consensus et de recueils de commentaires du processus ISO, la dernière version de l'ISO 31000 s'est considérablement améliorée depuis 2002. Certains points notables doivent encore être résolus, notamment, la terminologie utilisée non incluse (ISO/IEC Guide 73) avec la dernière version du ISO 31000 ; la pertinence de l'annexe A ; le positionnement des notions d'appétit du risque et d'aversion au risque dans une politique de risque ; et la notion même de management des risques* », explique Christopher Lajtha, fondateur d'Adageo, un cabinet de ressources en gestion des risques. Il ajoute qu'« *il est très important que la volonté originale de ne pas certifier le* guideline *ISO 31000 soit respectée* ».

PLUS DE CRÉDIBILITÉ POUR LES RISK MANAGERS

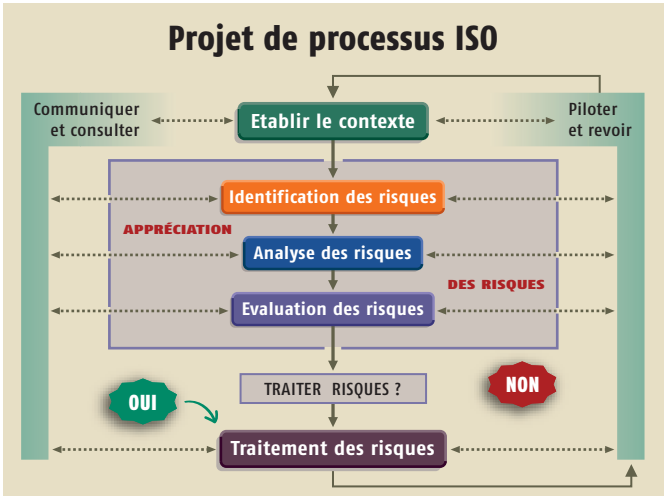
En France, les risk managers ont des profils très différents d'une entreprise à l'autre. Cependant, quelles que soient sa formation, ses responsabilités et ses compétences, le risk manager trouvera un outil de référence choisi sur lequel il pourra s'appuyer pour renforcer l'intégration du management du risque au sein de l'organisation.

L'existence de ce standard international plutôt que des normes nationales, lorsqu'elles existent, offre aux risk managers une plus grande crédibilité et une meilleure reconnaissance interne face aux autres fonctions traditionnelles de l'entreprise. La fonction apparaîtra comme plus structurée, renforçant son rôle de facilitateur et de communicateur, surtout s'il travaille pour une société internationale.

Le risk manager d'une grande société française nous avoue même qu'il attend impatiemment le standard ISO 31000 afin de renforcer sa crédibilité auprès de la direction de ses filiales aux Etats-Unis !

En tant que norme-cadre unique pour toutes les classes de risques et d'activités, elle devrait être accueillie favorablement par le secteur de l'assurance. L'inclusion du référentiel ISO dans les questionnaires d'assurance permettrait une meilleure mutualisation des risques dommages et RC des entreprises assurées. Les pays et organisations habitués au standard australien AS/NZS 4360 devraient adopter rapidement cette nouvelle norme, alors que d'autres auront plus de difficultés. « *Les entreprises devront adapter le référentiel à leur propre organisation en tenant compte de leurs spécificités culturelles et humaines* », explique Kevin Knight. •

**Atlascope, société de conseil en gestion des risques, lance début 2009 le site internet www.ISO31000.fr qui servira de portail d'information et d'échanges pour les entreprises et organisations françaises désireuses de mettre en place adéquatement ou d'adapter leur programme de gestion des risques (contact : iso31000@atlascope.fr). Parallèlement, Carm Institute a déjà incorporé l'ISO 31000 dans l'enseignement de la qualification professionnelle ARM (associé en risk management) en France.*



Source : Carm Institute

Position de Ferma

Dès 2004, Thierry Van Santen, alors président de Ferma (Federation of European Risk Management Associations) adopte le standard anglais rédigé conjointement par l'Airmic (équivalent britannique de l'Amrae, l'association française des risk managers), l'IRM (institut) et Alarm (secteur public). Dans sa prise de position datée du 22 juin 2007, Ferma soutient l'adoption d'un standard international en gestion des risques qui soit de haut niveau, court, utilisant le vocabulaire du guide ISO/IEC73, et non « certifiable ». Des contacts ont actuellement lieu au niveau européen avec le CEN et ses membres européens.