# LES CAHIERS DE LA SÉCURITÉ INDUSTRIELLE

2009-05

# LA NORME ISO 31000

## 10 QUESTIONS

GILLES MOTET

FonCSI
FONDATION POUR UNE CULTURE DE SÉCURITÉ INDUSTRIELLE

La *Fondation pour une Culture de Sécurité Industrielle* (FonCSI) est une Fondation de Recherche reconnue d'utilité publique par décret en date du 18 avril 2005. Elle a pour ambitions de :

- contribuer à l'amélioration de la sécurité dans les entreprises industrielles de toutes tailles, de tous secteurs d'activité ;
- rechercher, pour une meilleure compréhension mutuelle et en vue de l'élaboration d'un compromis durable entre les entreprises à risques et la société civile, les conditions et la pratique d'un débat ouvert prenant en compte les différentes dimensions du risque ;
- favoriser l'acculturation de l'ensemble des acteurs de la société aux problèmes des risques et de la sécurité.

Pour atteindre ces objectifs, la Fondation favorise le rapprochement entre les chercheurs de toutes disciplines et les différents partenaires autour de la question de la sécurité industrielle : entreprises, collectivités, organisations syndicales, associations. Elle incite également à dépasser les clivages disciplinaires habituels et à favoriser, pour l'ensemble des questions, les croisements entre les sciences de l'ingénieur et les sciences humaines et sociales.

Éditeur : **Institut pour une Culture de Sécurité Industrielle**
Association de loi 1901

http://www.icsi-eu.org/


**Fondation pour une Culture de Sécurité Industrielle**
Fondation de Recherche, reconnue d'utilité publique

http://www.icsi-eu.org/

6 allée Émile Monso – BP 34038
31029 Toulouse cedex 4
France

Téléphone : +33 (0) 534 32 32 00
Fax : +33 (0) 534 32 32 01
Courriel : contact@icsi-eu.org

# Avant-propos

La société se trouve face à deux objectifs qui semblent a priori contradictoires : développer l'innovation (nouvelles technologies, démarches et organisations, nouveaux produits, procédés et services, *etc.*) qui est source intrinsèque de risques, et garantir un haut niveau de sécurité aux citoyens. Pour réconcilier ces objectifs, les risques doivent être maîtrisés et les justifications de cette maîtrise fournies. De nombreux documents sectoriels proposent des moyens répondant à ces exigences. La nouvelle norme ISO 31000 fournit un cadre général au Management du risque qui englobe la problématique de la sécurité et l'inscrit au sein des multiples préoccupations des organismes et des autres parties prenantes. Elle propose une nouvelle définition du risque ; elle améliore le *processus de Management* du risque ; elle favorise l'intégration du Management du risque dans le *système de Management* de l'organisme ; elle introduit des principes qui pilotent les choix des activités de Management du risque. Ces apports permettent d'aborder de façon cohérente et explicite de nombreux aspects interférant généralement de façon anarchique et implicite dans les activités de Management du risque : multiplicité d'objectifs conflictuels, distribution des responsabilités, évaluation de l'efficacité des moyens et de leurs utilisations, *etc.*

Ce document fournit un éclairage sur cette norme, abordant ses origines et ses apports. Il n'a pas pour ambition d'en détailler le contenu et encore moins d'en proposer des mises en œuvre pratiques.

## À propos de l'auteur

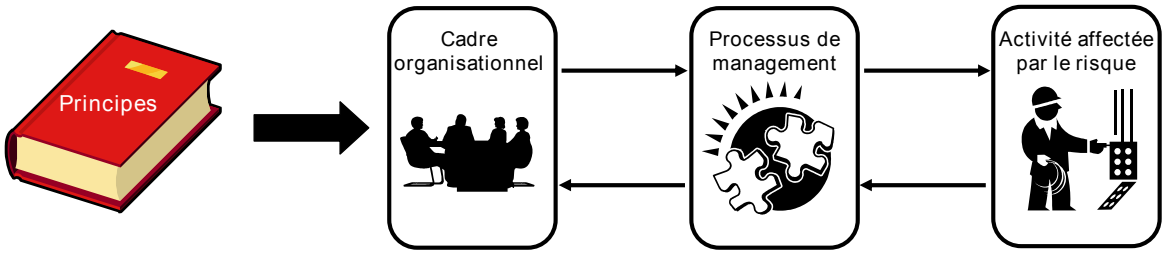
Gilles Motet est professeur à l'Institut National des Sciences Appliquées de Toulouse et chercheur au LATTIS (LAboratoire Toulousain de Technologie et d'Ingénierie des Systèmes). Sa recherche concerne les principes du Management du risque et leurs applications à la maîtrise des fautes dans les modèles logiciels et les programmes. Il est co-auteur d'ouvrages parus chez InterEditions, Kluwer et Prentice Hall sur la *Sûreté de fonctionnement des systèmes informatiques*. Il assure la Direction Scientifique de la *Fondation pour une Culture de Sécurité Industrielle* et de l'*Institut pour une Culture de Sécurité Industrielle*.

Il a participé aux travaux du groupe « Évaluation des risques » de l'AFNOR et a représenté la France dans le groupe de travail « Risk management » de l'ISO en charge de la rédaction de la norme ISO 31000 (« Risk Management - Principles and guidelines ») et de la révision du Guide 73 de l'ISO (« Risk Management - Vocabulary »). Il est à l'origine du Master « System Engineering » de l'INSA de Toulouse et du Mastère Spécialisé « Risk Engineering » co-accrédité par l'INSA et l'INP de Toulouse en collaboration étroite avec l'ICSI (*cf.* le Pôle des Mastères en Management des risques).

Pour tout commentaire ou remarque permettant d'améliorer ce document, merci d'envoyer un courriel à `cahiers@icsi-eu.org`.

# Table des matières






Le schéma conceptuel de la norme ISO 31000.

Question

1

10

# *Pourquoi une nouvelle norme en Management des risques ?*

Il existe de nombreuses normes ou documents métier concernant le Management des risques et sa déclinaison dans des domaines tels que la sécurité. Cependant, ces normes sont sectorielles (avionique, ferroviaire, nucléaire, procédés, pharmacie, *etc.*). De plus, elles concernent souvent des points de vue limités comme des étapes particulières du développement de projets (par exemple la conception). D'autres documents traitent de risques affectant des technologies spécifiques (par exemple le logiciel ou l'électronique). D'autres, enfin, répondent à des sources de dangers ciblées (par exemple, les explosions ou les rayonnements électromagnétiques).

Or, la gestion des risques de systèmes sociotechniques complexes comme une installation industrielle ou un développement de projet industriel, nécessite d'**aborder la question des risques d'un point de vue global**. Ainsi, même si chaque domaine a développé des terminologies et des techniques d'usage partiel et spécifique, il existe des problématiques qui requièrent une approche globale et générique.

Par ailleurs, on constate que les ingénieurs ont parfois une perte de repères lorsqu'ils appliquent les standards sectoriels. Ils peinent à les positionner dans une approche de Management des risques globale à l'organisme et ainsi à bien comprendre les apports – mais aussi les limites – de l'application de ces documents.

La nouvelle norme ISO 31000 a tiré profit des échanges entre des experts internationaux issus d'organismes très variés (industriels, administrations, ONG, *etc.*) relevant de multiples secteurs d'activités. Elle favorise **la prise en compte des risques par l'ensemble de l'organisme** et fournit aux parties prenantes **l'assurance d'une meilleure maîtrise de ces risques**.

L'ISO 31000 est une « norme chapeau » permettant d'**établir un dialogue entre les secteurs d'activité** en leur proposant un vocabulaire et un cadre commun. Cette norme **facilitera également le développement des formations** dans le domaine de la gestion des risques qui était jusqu'alors rendu difficile par l'impossibilité de multiplier les présentations de pratiques sectorielles.

# *Qu'est-ce que l'ISO 31000 ?*

2

10

Question

L'ISO 31000 propose une approche générique du Management des risques mais ne préconise pas de moyens opérationnels de mise en œuvre. Cette norme suggère de **bonnes questions** pour aborder le sujet complexe de la gestion des risques **et non de bonnes pratiques** pour y répondre. Les moyens de mise en œuvre du Management des risques sont développés dans les documents métiers sectoriels qui ne sont donc pas rendus obsolètes par cette norme. Ils y trouvent au contraire un vocabulaire et un cadre global pour les situer.

L'ISO 31000 ne concerne pas exclusivement les grands groupes industriels ou financiers ou les grandes administrations publiques, mais **tout type d'organisme, de tous secteurs et de toutes tailles** (entreprise, gouvernement, ONG, individu, *etc.*). Ses principes stipulent d'ailleurs que sa mise en œuvre doit être adaptée aux caractéristiques de l'organisme (taille, type de risque traité, *etc.*). Elle n'a donc pas pour but d'uniformiser les pratiques, mais d'**harmoniser les démarches** en termes de principes et de processus.

L'ISO 31000 fournit tout d'abord **une redéfinition du terme de risque** qui permet de prendre en compte explicitement de nombreuses problématiques récentes (*cf.* question 3).

Le *processus de Management des risques* qu'elle propose, complète ceux existants en y intégrant par exemple **la prise en compte explicite du contexte** dans lequel le risque est étudié (*cf.* question 4).

La norme introduit un second processus appelé *Cadre organisationnel* structurant les activités des organismes pour **mettre en place et améliorer continûment le *processus de Management des risques*** (*cf.* question 5).

Enfin, **elle base l'ensemble de ces activités sur des *principes*** généraux qui doivent régir la structure de ces processus et leur mise en œuvre (*cf.* question 6).

L'ISO 31000 est structurée en 4 grandes sections : la première définit le *vocabulaire* employé dans la norme, la seconde établit les *principes*, la troisième décrit le *cadre organisationnel* et la quatrième expose le *processus de Management des risques*. Une vue schématique en est fournie à la page *vii*.

Question

3

10

# *Pourquoi avoir redéfini la notion de risque ?*

Durant de très nombreuses années, le concept de « risque » a été assimilé à celui de ***danger***. Sa maîtrise était du ressort des **techniciens** qui comprenaient les mécanismes, par exemple physico-chimiques, pouvant entrainer des accidents. L'occurrence des dommages était prévenue par des **traitements à la source** ayant pour but de réduire ce danger.

Cette approche conduisait implicitement à l'ignorance totale ou partielle des effets positifs de l'activité source du risque. Pour tenir compte de ces apports tout en prévenant les dommages potentiels, la définition du terme « risque » s'est ensuite déplacée vers celle d'***événement probable ayant des conséquences***. La présence d'une source de risque était rendue acceptable au regard des très improbables dommages qu'elle pouvait engendrer et des contributions positives qu'elle fournissait assurément. La gestion des activités médicales, des produits pharmaceutiques ou encore des moyens de transports ou des installations industrielles, relève actuellement de cette approche. Elle donne lieu à l'établissement de modèles d'analyse probabiliste des effets mis au point par des **ingénieurs** et à l'intégration de **barrières** pour réduire la vraisemblance et l'importance des effets indésirés potentiels.

La norme ISO 31000 définit le risque comme l'***effet de l'incertitude sur l'atteinte des objectifs***. Cette définition déplace de nouveau la question du risque en imposant de spécifier les objectifs d'une activité dont l'atteinte pourrait être entravée par l'occurrence de circonstances incertaines. « Améliorer la santé à des coûts raisonnables dans un contexte donné » est un exemple introduisant trois objectifs : améliorer la santé, en respectant une enveloppe budgétaire, sans bouleverser le contexte social. Cette multiplicité des objectifs nécessite que les **décideurs** fassent des **arbitrages**. Ces derniers devront être pris en compte par les ingénieurs et les techniciens proposant des moyens empêchant que les effets de l'incertitude n'entravent le déroulement des activités mises en place pour atteindre les objectifs.

Cette nouvelle définition ne remet pas en cause les problématiques de traitement des dangers ou d'analyse des événements dommageables. Elle les complète en **formalisant l'importance du rôle des décideurs**, qu'il s'agisse de personnes physiques ou morales (directeurs de sites industriels, élus, autorités de contrôle, ingénieurs, *etc.*) ou plus généralement de la société. Elle permet tout d'abord de signifier un état de fait, à savoir que les objectifs sont multiples, qu'ils concernent non seulement la sécurité mais aussi des questions économiques et politiques, personnelles ou sociétales. Les énoncer évite de parasiter les activités de Management des risques par des non-dits et, en formulant explicitement les arbitrages, **rend plus transparentes les nombreuses décisions prises** durant ces activités.

# *Quels changements dans le processus de Management du risque ?*

4

10

Question

Le processus générique de Management des risques proposé dans l'ISO 31000 reprend les activités classiques d'appréciation des risques (identification, analyse, évaluation) et de leur traitement. La norme les complète par 3 autres activités.

L'**Établissement du contexte** oblige à définir en amont de ces activités, les paramètres fondamentaux caractérisant l'environnement dans lequel s'effectue le Management du risque et les valeurs de ces paramètres. L'environnement est tout d'abord externe à l'organisme. Des seuils stipulés par une réglementation ou des critères d'appréciation des risques issus des parties prenantes, sont deux exemples de paramètres. L'environnement du Management du risque inclut également l'organisme lui-même (la norme parle d'environnement interne). Les pratiques propres à l'organisme en sont des exemples de paramètres. La norme propose d'énumérer ces paramètres et de séparer leur définition de leurs utilisations dans les autres tâches du processus, clarifiant ainsi les différentes responsabilités des intervenants dans le *processus de Management du risque*. Par exemple, la *matrice de risque* constitue un paramètre utilisé lors de l'évaluation du risque. Ses valeurs ne doivent pas être définies par les personnes effectuant cette évaluation. En effet, elles caractérisent, entre autres, l'importance relative entre la probabilité d'occurrence d'événements dommageables et la gravité des dommages. Il s'agit donc d'une donnée relative au contexte dans lequel s'effectue l'évaluation des risques. D'autres valeurs de cette matrice, voire un autre moyen d'évaluation, sont utilisés dans d'autres contextes.

La norme met également en valeur la tâche de **Communication et concertation** et son couplage avec l'ensemble des autres tâches du processus. Ces échanges concernent aussi bien les parties prenantes externes que celles internes à l'organisme qui gère le risque. La norme mentionne en particulier que cette tâche facilite la compréhension du contexte et l'intégration de ses changements par les activités de Management des risques.

Elle distingue enfin la tâche intitulée **Surveillance et revue** ayant par exemple pour but de ré-évaluer le déroulement des activités de Management des risques. Cette tâche peut ainsi mesurer l'efficacité de l'emploi des moyens mis en œuvre afin d'améliorer leurs utilisations futures.

Question 5 sur 10

# *Qu'est-ce que le Cadre organisationnel ?*

La gestion des risques est fréquemment mise en œuvre par plusieurs *processus de Management des risques*, qui sont déroulés en parallèle afin de répondre à divers objectifs tels que la prévention des événements accidentels, d'une part, et la prévention des dommages dus à la malveillance, d'autre part. Or ces processus peuvent présenter **des enjeux conflictuels** qu'il convient de gérer non pas *a posteriori* mais *a priori*. Par exemple, la mise en œuvre de la tâche de « Communication et concertation », pour répondre à des besoins de prévention des accidents (c'est–à–dire sécurité au sens *safety*) conduira à diffuser largement des informations sur les dangers, leurs effets potentiels et les moyens mis en œuvre pour les maîtriser. Cette communication est parfois obligatoire, comme pour les « résumés non-techniques » des études de dangers. Une telle communication peut aller à l'encontre des objectifs de prévention des malveillances (c'est–à–dire sécurité au sens *security*). Or une installation industrielle, par exemple, doit atteindre simultanément ces deux objectifs (*safety* et *security*).

Le *Cadre organisationnel* (« Framework » en anglais) a pour but de gérer ces conflits et, de façon plus large, d'**intégrer les activités de Management du risque dans celles de l'organisme**. En effet, la gestion des risques ne doit pas être traitée comme une activité autonome, mais au contraire associée aux autres activités dont celles opérationnelles. Elle doit ainsi être utile à ces activités et notamment contribuer aux décisions qu'elles nécessitent.

Ce *Cadre organisationnel* est lui-même défini par un processus qui **permet la mise en place des *processus de Management des risques* ainsi que leur amélioration continue**. Le premier aspect concerne par exemple le choix de moyens efficaces pour réaliser les activités des *processus de Management des risques*. Le second (amélioration continue) nécessite la mise en place de **dispositifs d'évaluation** de ces moyens et leur adaptation permanente. Le processus du *Cadre organisationnel* est constitué d'un cycle de type PDCA (Plan, Do, Check and Act) bien connu en Qualité. Il est précédé par une tâche imposant de définir, entre autres, **les objectifs et les indicateurs de performance du Management du risque**. Intitulée « Mandat et engagement », cette tâche marque l'importance du « leadership » dans le Management du risque.

Le *Cadre organisationnel* regroupe des activités permettant donc de mettre en place **une approche proactive du Management des risques** intégrant les connaissances nouvelles (données, modèles, techniques, pratiques, *etc.*), par une évaluation continue de l'efficacité des moyens utilisés et par une veille sur les moyens nouveaux disponibles.

# *Pourquoi ériger des principes sur le Management du risque ?*

6

10

Question

Les implantations des *processus de Management du risque* sont issues des activités du *Cadre organisationel*. La norme ISO 31000 base la réalisation de ce cadre et donc des processus sur **onze « Principes »**. Il est important de mentionner que ces principes ne concernent pas les risques particuliers à gérer mais affectent la façon de les gérer. Les questions telles que « Quel est le niveau de risque acceptable ? » relèvent de l'« Établissement du contexte » de chaque *processus de Management du risque*.

Par exemple, la norme érige en principe que « **le Management des risques doit créer de la valeur** ». Cette phrase ne doit pas être interprétée d'un point de vue financier. Elle exprime que l'ensemble des activités de gestion des risques mises en place doivent contribuer efficacement à l'atteinte des objectifs de l'organisme afin de maîtriser les effets de l'incertitude. Ce principe induit notamment les activités d'évaluation des moyens du *processus de Management des risques* par le *Cadre organisationnel* et l'évaluation de l'efficacité de l'utilisation de ces moyens par le *processus de Management des risques* lui-même. Par exemple, elle pourrait conduire à évaluer l'efficacité réelle d'une réglementation avant de la promulguer. Des techniques comme l'Analyse Coût-Bénéfices pourraient être utilisées comme outil d'évaluation.

Un second principe stipule que « **le Management des risques traite explicitement de l'incertitude** ». Cette incertitude concerne par exemple les connaissances sur les sources du risque. Les modèles et outils d'analyse doivent donc prendre en compte cette méconnaissance. L'acceptation de l'incertitude induit également l'aspect itératif du *processus de Management du risque* afin d'intégrer les nouvelles connaissances disponibles. L'incertitude affecte aussi les moyens utilisés pour gérer le risque, comme ceux concernant son analyse et son traitement (par exemple l'efficacité des barrières de protection). L'impact de l'incertitude sur les usages de ces moyens doit être explicité.

Le principe qui énonce que « **le Management du risque doit intégrer les facteurs humains et culturels** » est par exemple pris en compte dans la tâche « Mandat et engagement » du *Cadre organisationnel*. En effet, elle requiert de s'assurer de la disponibilité des ressources humaines adéquates. Dans le *processus de Management des risques*, ce principe impacte, entre autres, la mise en œuvre de la tâche d'« Établissement du contexte ». Par exemple, celle-ci doit identifier les critères d'appréciation des risques adoptés par les parties prenantes.

L'explicitation des principes qui régissent le Management des risques est essentielle. En effet, ces principes vont induire la façon de gouverner toutes les activités. L'organisme devrait donc au préalable stipuler son degré d'adhésion à ces principes.

Question

7

10

# *À qui cette norme est-elle destinée ?*

De nombreuses personnes interviennent dans les diverses activités de Management des risques. La norme ISO 31000 s'adresse à chacune d'elles qui en tirera des profits différents.

**Les personnes en charge de la mise en place des activités de Management des risques au sein des organismes** trouveront dans cette norme un cadre précisant les questions à aborder et proposant une structure pour les traiter : principes, cadre organisationnel, processus de Management. Cette norme s'adresse donc en premier lieu aux directions sécurité des sociétés mais aussi aux autorités de tutelle (ministères, agences, *etc.*).

**Les personnes définissant des pratiques** (modèles, techniques, outils, guides, *etc.*) pourront positionner celles-ci dans un canevas générique. Les objectifs auxquels répondent ces pratiques seront ainsi précisés, limitant clairement les contributions à attendre de celles-ci. Ces personnes identifieront en outre plus précisément les activités nécessitant l'élaboration de nouveaux moyens et les besoins auxquels ils doivent répondre. Cette norme s'adresse donc également aux rédacteurs de normes sectorielles, aux développeurs de bonnes pratiques (guides ou procédures) ou aux créateurs de techniques ou d'outils.

**Les personnes chargées de gérer des risques particuliers** disposeront d'un cadre commun permettant de situer leurs activités et les pratiques qu'elles mettent en œuvre. Elles connaitront ainsi mieux les rôles et responsabilités de chacun dans la réalisation des multiples tâches indispensables à une gestion efficace des risques.

**Les personnes chargées d'évaluer les pratiques** des organismes en matière de Management des risques comme les autorités de contrôle (organismes de certification, d'autorisation d'exploiter, *etc.*), disposeront d'une structure générique permettant de situer les pratiques effectives.

L'ISO 31000 fournit donc aux divers intervenants dans la gestion des risques, une démarche structurée qui peut être partagée, tout en permettant de préciser les missions de chacun sur l'ensemble de ces activités.

# *Par qui et comment cette norme a-t-elle été écrite ?*

8

10

Question

La sphère des rédacteurs de normes est souvent perçue comme un milieu regroupant des vieux messieurs se chamaillant sur la place d'une virgule car d'accord sur l'essentiel. Cette vision est erronée dans le cas général et tout particulièrement fausse concernant le groupe des experts ayant élaboré l'ISO 31000.

Tout d'abord, la rédaction de cette norme a été **un choc de cultures** entre des personnes issues de secteurs très variés : sécurité des installations industrielles et des produits, finance, gestion de projet, santé publique, organisations de défense de l'environnement, *etc.* Les discussions n'ont pas porté sur des désaccords syntaxiques mais sur **des visions diverses de ce qu'est le risque et sur la façon de l'aborder**. Par exemple, un terme comme l'« appétit du risque » faisait frémir les uns alors qu'il constituait un mot commun pour d'autres. En effet, un sens positif est donné au risque dans le secteur financier, alors qu'une connotation négative est souvent adoptée dans le domaine de la sécurité. Le terme « attitude face au risque » a permis d'y intégrer la notion d'« aversion au risque ».

Les points de vue sur le risque et sur sa gestion sont éminemment culturels et ceci même dans un secteur donné. Un latin n'a pas la même approche qu'un anglo-saxon ou qu'un asiatique. Ces cultures se sont également confrontées pour donner lieu à un texte reflétant cette diversité. Le résultat a été obtenu dans un délai relativement bref. Les travaux lancés en juin 2004 ont été conclus fin 2008. Cette norme n'est assurément **pas le fruit de compromissions mais celui d'un consensus**. Les différents secteurs industriels, publics, associatifs, des divers pays ont contribué à enrichir son contenu tant au niveau national (via l'AFNOR) qu'international (à l'ISO).

Le résultat de ce travail aura, je l'espère, comme premier effet de **permettre à chacun de requestionner son point de vue** sur le concept de risque et sur ses approches pour l'aborder, et d'améliorer *in fine* ses pratiques de Management du risque.

À titre personnel, il me reste à l'esprit les nombreux sujets débattus, les arguments avancés et les accords qui ont conduit à la rédaction de la norme.

Question

9

10

# *Quels travaux futurs ?*

Cette nouvelle norme va tout d'abord **nécessiter d'informer et de former** non seulement sur son contenu mais aussi sur la vision qu'elle sous-tend. Nous avons par exemple mentionné la nouvelle définition du risque à la question 3. L'importance de l'« Établissement du contexte » dans le *processus de Management des risques*, l'introduction du *Cadre organisationnel* et l'expression de *Principes* régissant l'ensemble, devront être expliquées afin de faire comprendre leurs intérêts.

Comme mentionné en réponse à la question 1, l'ISO 31000 propose une approche générale du Management des risques alors que des pratiques existent déjà. L'objet de cette nouvelle norme n'est pas de balayer les normes sectorielles, ni les documents métiers qui proposent ces pratiques. L'étude de leur intégration dans cette « norme chapeau » permettra de **positionner les pratiques existantes** et, éventuellement, de **mettre en valeur les aspects non couverts** par celles-ci afin d'y porter remède.

De nombreux secteurs disposent de documents propres demandant l'usage de moyens généralement proches voire souvent similaires. La création de l'ISO 31000 peut être une opportunité d'un rapprochement de ces secteurs afin de disposer d'un vocabulaire commun et d'**harmoniser les démarches en tirant profit des expériences de chacun**.

En plus d'aspects classiques, comme ceux du *processus de Management des risques*, qu'elle complète (tâche « Établissement du contexte »), l'ISO 31000 introduit ou du moins formalise de **nouvelles questions** essentiellement à travers ses *Principes* et son *Cadre organisationnel*. Les pratiques associées restent souvent à définir. De nouveau, de nombreux travaux inter-sectoriels pourraient être conduits afin de réduire les coûts de ces études et de partager les expériences. Cela pourrait être le cas par exemple de l'évaluation des performances de divers moyens de modélisation et d'analyse de l'incertitude.

L'idée d'une boucle d'amélioration continue sous-tendue par le *Cadre organisationnel* pourrait conduire à se questionner sur **la définition de niveaux de maturité des organismes** devant gérer des risques et sur **les moyens de progrès** permettant de passer d'un niveau à l'autre. Cet accès progressif à un haut niveau de maîtrise des risques serait assurément utile aux organismes, et en particulier aux PME, et faciliterait l'appréciation des parties prenantes (administration, ONG, *etc.*). Cette question est cependant très sensible.

# *L'ISO 31000 : une évolution ou une révolution ?*

10

Question 10

L'ISO 31000 sera certainement perçue tout d'abord comme une évolution dans le Management des risques en s'attachant aux éléments méthodologiques qu'elle propose : le processus du *Cadre organisationnel* et le *processus de Management du risque*. Du recul sera sans doute nécessaire pour assimiler les remises en cause qu'elle sous-tend. Essayons d'en anticiper quelques-unes.

La nouvelle norme définit le risque comme l'« effet de l'incertitude sur l'atteinte des objectifs ». Nous avons mis en valeur à la question 3, l'évolution du concept de risque et introduit son impact sur les approches de Management du risque. Cette nouvelle définition va déplacer les débats sur le risque vers la question fondamentale : **quels sont les objectifs de l'organisme ou des autres parties prenantes ?** La formulation explicite de ces objectifs amènera sans doute des débats. En effet, ces objectifs sont multiples et souvent contradictoires. Par exemple, nous voulons des emplois et consommer des produits manufacturés, mais pas de sites industriels. Nous désirons que notre activité soit proche de notre domicile, mais que celle des autres en soit la plus éloignée possible. **Des arbitrages devront être effectués entre ces différents objectifs**. La norme suggère qu'ils soient explicites et justifiés. Sommes-nous prêts à le faire ? Cette définition initiale des objectifs et l'explicitation des arbitrages devraient faciliter les autres activités de Management des risques et rendront plus transparentes et mieux comprises les décisions.

La norme incite à expliciter également **les rôles et responsabilités de chacun** dans le Management des risques. Ainsi, la tâche d'« Établissement du contexte » du *processus de Management du risque* permet de délimiter la portée des activités suivantes de ce processus. Elle affirme que la gestion des risques dépendra tout d'abord des réglementations mais aussi des parties prenantes externes, de leurs attentes, valeurs, cultures, *etc.* Elle souligne également que cette gestion des risques dépendra aussi du contexte interne à l'organisme : sa structure, ses normes et pratiques, ses savoir-faire, mais aussi ses valeurs. De même, la tâche « Mandat et engagement » du *Cadre organisationnel* définit **les responsabilités incombant à la direction, dont celle d'expliciter les objectifs**. La tâche « Conception du cadre organisationnel de Management des risques » doit, par exemple, définir les moyens tels que les processus, méthodes, modèles et outils qui seront utilisés dans les tâches du *processus de Management des risques*. Ceci permet de **séparer explicitement les responsabilités de choisir les bons moyens** (rôle du *Cadre organisationnel*) **et celles de bien utiliser ces moyens** (rôle du *processus de Management des risques*).

Le *Cadre organisationnel* n'est pas un « Système de Management » mais une approche pour **intégrer les pratiques du Management du risque dans le Système de Management existant** dans l'organisme. Nous avons mentionné que son processus itératif permet une amélioration continue du *processus de Management des risques*. Ce fait revient à **accepter l'imperfection des activités de ce processus**, même s'il met en œuvre les meilleures connaissances à un moment donné. L'aspect perfectible des activités du processus revient implicitement à accepter l'occurrence d'incidents ou d'accidents qui doivent être sources de progrès. Si cette approche est réaliste, est-elle audible aujourd'hui ? Quelle révolution implique-t-elle dans les relations entre les parties prenantes de la gestion des risques ? Je pense en particulier aux médias et à la justice.

## Reproduction de ce document

Ce document est diffusé selon les termes de la license BY-NC-ND du Creative Commons. Vous êtes libres de reproduire, distribuer et communiquer cette création au public selon les conditions suivantes :

- **Paternité**. Vous devez citer le nom de l'auteur original de la manière indiquée par l'auteur de l'œuvre ou le titulaire des droits qui vous confère cette autorisation (mais pas d'une manière qui suggérerait qu'ils vous soutiennent ou approuvent votre utilisation de l'œuvre).
- **Pas d'utilisation commerciale**. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.
- **Pas de modification**. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

Vous pouvez télécharger ce document (et d'autres versions des *Cahiers de la Sécurité Industrielle*) au format PDF depuis le site web de la FonCSI.



**Fondation pour une Culture de Sécurité Industrielle**
Fondation de Recherche reconnue d'utilité publique
http://www.icsi-eu.org/

6 allée Émile Monso – BP 34038
31029 Toulouse cedex 4
France

Téléphone : +33 (0) 534 32 32 00
Fax : +33 (0) 534 32 32 01
Courriel : contact@icsi-eu.org


6 allée Emile Monso
Zac du Palays - BP 34038
31029 Toulouse Cedex 4
www.icsi-eu.org