RAPPORT TECHNIQUE

ISO/TR 31004

Première édition
2013-10-15

Management du risque — Lignes directrices pour l'implementation de l'ISO 31000

Risk management — Guidance for the implementation of ISO 31000

Numéro de référence
ISO/TR 31004:2013(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2014

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour l'élaboration du présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/CEI, Partie 1. Il convient, en particulier, de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/CEI, Partie 2 (voir www.iso.org/directives).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou sur la liste ISO des déclarations de brevets reçues (voir www.iso.org/patents).

Les éventuelles appellations commerciales utilisées dans le présent document sont données pour information à l'attention des utilisateurs et ne constituent pas une approbation ou une recommandation.

Pour une explication de la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité et pour toute information au sujet de l'adhésion de l'ISO aux principes de l'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: Avant-propos — Informations supplémentaires Foreword - Supplementary information

Le Comité responsable du présent document est le Comité technique ISO/TC 262, *Management du risque*.

Introduction

0.1 Généralités

Les organismes utilisent différentes méthodes pour gérer les effets de l'incertitude sur leurs objectifs, c'est-à-dire pour gérer le risque, en détectant et comprenant le risque et en le modifiant au besoin.

Le présent Rapport technique est destiné à aider les organismes à améliorer l'efficacité de leurs actions de management du risque en les alignant sur l'ISO 31000:2009. L'ISO 31000 présente une approche générique de management du risque qui peut être appliquée à tous les organismes pour leur permettre d'atteindre leurs objectifs.

Le présent Rapport technique est destiné à être utilisé par ceux qui, au sein des organismes, prennent les décisions qui influent sur la réalisation de leurs objectifs, notamment les responsables de la gouvernance et ceux qui fournissent aux organismes conseils et accompagnement en matière de management du risque. Le présent Rapport technique est également destiné à être utilisé par toute personne intéressée par le risque et son management, y compris les enseignants, les étudiants, les législateurs et les régulateurs.

Le présent Rapport technique est destiné à être lu conjointement avec l'ISO 31000 et s'applique à tous les types et à toutes les tailles d'organismes. Les concepts fondamentaux et les définitions qui sont essentiels à la compréhension de l'ISO 31000 sont expliqués à l'Annexe A.

L'Article 3 propose une méthodologie générique pour permettre aux organismes d'aligner leurs propres dispositions de management du risque sur l'ISO 31000, de manière planifiée et structurée. Elle propose également un mécanisme d'ajustement dynamique lorsque des modifications surviennent dans l'environnement intérieur et extérieur de l'organisme.

D'autres annexes fournissent des conseils, des exemples et une explication concernant la mise en œuvre d'aspects choisis de l'ISO 31000, afin d'assister les utilisateurs du présent Rapport technique en fonction de leur expertise et de leurs besoins particuliers.

Les exemples figurant dans le présent Rapport technique peuvent ou non être directement applicables à des situations ou à des organismes donnés. Ils sont fournis à titre d'exemple uniquement.

0.2 Concepts et principes sous-jacents

Certains mots et concepts sont fondamentaux pour comprendre tant l'ISO 31000 que le présent Rapport technique: ils sont expliqués dans l'ISO 31000:2009, Article 2, ainsi qu'à l'Annexe A du présent Rapport technique.

L'ISO 31000 énumère onze principes sous-tendant un management du risque efficace. Ces principes servent à définir et à éclairer tous les aspects de l'approche du management du risque de l'organisme. Les principes décrivent les caractéristiques d'un management du risque efficace. Plutôt que de se limiter à mettre en œuvre ces principes, il est important que l'organisme les incorpore à tous les aspects du management. Ils servent d'indicateurs de performance du management du risque et renforcent la valeur pour l'organisme d'un management efficace du risque. Ils influencent également tous les éléments du processus de transition décrit dans le présent Rapport technique et les points techniques qui font l'objet de ses annexes. D'autres conseils sont donnés dans l'Annexe B.

Dans le présent Rapport technique, les termes «direction générale» et «organe de surveillance» sont tous deux utilisés: «direction générale» se réfère à la personne ou au groupe de personnes qui dirige et pilote un organisme au plus haut niveau, alors que «organe de surveillance» se rapporte à la personne ou au groupe de personnes qui gouverne un organisme, définit des orientations et à qui la direction rend des comptes.

NOTE Dans de nombreux organismes, l'organe de surveillance peut être dénommé conseil d'administration, conseil des administrateurs, conseil de surveillance, etc.

Management du risque — Lignes directrices pour l'implementation de l'ISO 31000

1 Domaine d'application

Le présent Rapport technique propose aux organismes des lignes directrices de management efficace du risque par la mise en œuvre de l'ISO 31000:2009. Il présente:

— une approche structurée permettant aux organismes d'adapter leurs dispositions en matière de management du risque pour les rendre conformes à l'ISO 31000, tout en tenant compte des caractéristiques de l'organisme;

— une explication des concepts sous-jacents de l'ISO 31000;

— des lignes directrices sur les aspects des principes et du cadre organisationnel de management du risque qui sont décrits dans l'ISO 31000.

Le présent Rapport technique peut être appliqué par tout public, toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu.

NOTE Pour plus de facilité, les différents utilisateurs de la présente Norme internationale sont désignés par le terme générique «organisme».

Le présent Rapport technique n'est pas spécifique à une industrie ou à un secteur, ni à un type de risque en particulier: il peut s'appliquer à toutes les activités et à toutes les composantes de tous les organismes.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 31000:2009, *Management du risque — Principes et lignes directrices*

3 Mise en œuvre de l'ISO 31000

3.1 Généralités

Le présent article propose des lignes directrices aux organismes souhaitant aligner leur approche et leurs pratiques de management du risque sur l'ISO 31000 et maintenir cet alignement de manière constante.

Il propose une méthodologie générale pouvant être appliquée, de manière planifiée, par tout organisme quelle que soit la nature de ses dispositions du moment en matière de management du risque. Cette méthodologie implique de:

— comparer les pratiques du moment avec celles décrites dans l'ISO 31000;

— identifier les changements nécessaires, préparer et mettre en œuvre un plan de réalisation de ces changements;

— maintenir une surveillance et des revues constantes pour veiller à l'actualisation et l'amélioration continue.

Ceci permettra à l'organisme de bénéficier d'une compréhension immédiate et exhaustive de ses risques et de s'assurer que ces risques sont cohérents avec son attitude face au risque et à ses critères de risque.

Indépendamment des raisons motivant la mise en œuvre de l'ISO 31000, celle-ci est supposée permettre à un organisme de mieux gérer ses risques afin de réaliser ses objectifs. Tous les organismes gèrent des risques dans une certaine mesure. Il convient que la stratégie de mise en œuvre de l'ISO 31000 identifie la façon dont l'organisme gère déjà le risque. Le processus de mise en œuvre, tel que décrit en 3.2, évalue les dispositions existantes et, si nécessaire, les adapte et les modifie pour les aligner sur l'ISO 31000.

L'ISO 31000 définit les divers éléments d'un cadre organisationnel de management du risque. Plusieurs avantages peuvent découler de l'intégration des éléments de ce cadre organisationnel à la gouvernance, aux fonctions et aux processus de l'organisme. Ils touchent à l'efficacité organisationnelle, à la prise de décisions judicieuses et à l'efficience.

a) Il convient de réaliser le cadre organisationnel de management du risque en intégrant ses éléments au système global de management et de prise de décision de l'organisme, que ce système soit formel ou informel; les processus de management existants peuvent être améliorés à la lumière de l'ISO 31000.

b) La compréhension et le management de l'incertitude deviennent un élément à part entière du (des) système(s) de management, permettant à l'organisme d'adopter une approche commune.

c) La mise en œuvre du processus de management du risque peut être adaptée proportionnellement à la taille et aux exigences de l'organisme.

d) La gouvernance (c'est-à-dire la direction et la surveillance) de la politique de management du risque, du cadre organisationnel et du (des) processus peut être intégrée aux dispositions existantes de l'organisme en matière de gouvernance.

e) Le rapport de management du risque est intégré aux autres rapports de management.

f) La performance du management du risque devient partie intégrante de l'approche globale des performances.

g) L'interaction et la connexion entre les domaines de management du risque souvent séparés d'un organisme (par exemple le management du risque d'entreprise, le management du risque financier, le management du risque projet, le management de la santé et de la sécurité, le management de la poursuite de l'activité, le management des assurances) peuvent être assurées ou améliorées, car dorénavant l'attention se cristallisera avant tout sur une définition et une réalisation des objectifs de l'organisme tenant compte du risque.

h) La communication sur l'incertitude et le risque entre les équipes de management et entre les niveaux hiérarchiques est améliorée.

i) Les différents silos de l'activité de management du risque d'un organisme se concentrent sur la réalisation des objectifs organisationnels dans un but commun. Il peut se dégager des avantages sociétaux indirects, les parties prenantes externes à l'organisme pouvant être encouragées à améliorer leur propre activité de management du risque.

j) Le traitement du risque et les moyens de maîtrise du risque peuvent devenir partie intégrante des actions quotidiennes.

3.2 Comment mettre en œuvre l'ISO 31000

Bien que l'ISO 31000 explique comment gérer efficacement le risque, elle n'explique pas comment intégrer le management du risque aux processus de management de l'organisme. Même si les organismes sont différents, même si leur situation de départ diffère, il existe une approche générique et systématique de mise en œuvre applicable à tous les cas.

Il convient que l'organisme détermine s'il est nécessaire d'apporter des changements à son cadre organisationnel de management du risque existant, avant de planifier et de mettre en œuvre ces

changements, puis de surveiller la constance de l'efficacité du nouveau cadre organisationnel. Cela permettra à l'organisme:

— d'aligner ses activités de management du risque sur les principes de management efficace du risque décrits dans l'ISO 31000:2009, Article 3;

— d'appliquer le processus de management du risque décrit dans l'ISO 31000:2009, Article 5;

— de satisfaire aux attributs d'un management de risque élevé de l'ISO 31000:2009, Article A.3;

— et ainsi d'atteindre les points principaux de l'ISO 31000:2009, Article A.2.

Cette approche s'applique également aux organismes qui sont déjà en phase avec l'ISO 31000, mais qui souhaitent améliorer en permanence leur cadre organisationnel et le processus de management du risque comme le recommande l'ISO 31000:2009, 4.6 et 5.6.

Tous les aspects de la transition peuvent être facilités en tirant des enseignements de l'expérience d'autres organismes qui gèrent des types de risques semblables ou qui ont entrepris un processus similaire.

3.3 Intégration de l'ISO 31000 aux processus de management de l'organisme

3.3.1 Généralités

L'ISO 31000 présente un cadre organisationnel et un processus générique de management du risque pour tout ou partie de n'importe quel type d'organisme. Le présent paragraphe fournit des lignes directrices pour intégrer les éléments de l'ISO 31000 à une approche de management de l'organisme, incluant ses activités, ses processus et ses fonctions. Les organismes peuvent choisir d'intégrer les concepts de l'ISO 31000 à leurs processus existants ou bien décider de concevoir et d'établir une nouvelle approche fondée sur l'ISO 31000. Le présent paragraphe décrit les éléments clés du cadre organisationnel et du processus, ainsi que les actions nécessaires à une intégration réussie de ces éléments permettant d'atteindre les objectifs organisationnels. Il existe de nombreuses façons d'intégrer l'ISO 31000 au sein d'un organisme. Il convient d'adapter le choix et l'agencement des éléments aux besoins de l'organisme et de ses parties prenantes. En appliquant ces lignes directrices, il convient de veiller à s'assurer que l'intégration soutient la stratégie d'ensemble du management de l'entreprise. Elle motive les efforts permettant d'atteindre les objectifs de l'organisme en matière de préservation et de création de valeur. Cette approche nécessite également de tenir compte de la culture de l'organisme, ainsi que de ses méthodologies de management du changement et des projets.

Le présent paragraphe décrit les éléments clés du cadre organisationnel et du processus, ainsi que les actions nécessaires à une intégration réussie de ces éléments permettant d'atteindre les objectifs organisationnels.

La mise en œuvre de l'ISO 31000est un processus dynamique, itératif et continu. L'implémentation du cadre organisationnel est, en outre, interconnectée avec le processus de management du risque décrit dans l'ISO 31000:2009, Article 5. La réussite se mesure à la fois en termes d'intégration du cadre organisationnel et en termes d'amélioration continue du management du risque à tous les niveaux de l'organisme.

L'intégration s'opère dans un contexte dynamique. Il convient que l'organisme surveille les changements suscités par le processus d'implémentation, mais aussi les changements opérés dans son contexte interne et externe. Cela peut inclure le besoin d'une modification de ses critères de risque.

3.3.2 Mandat et engagement

Toute activité de management commence par une analyse de la raison d'être des processus et de leurs étapes, ainsi que par une analyse coût-bénéfice. Il s'ensuit une décision de la direction générale et de l'organe de surveillance de mettre en œuvre et de fournir l'engagement et les ressources nécessaires.

Typiquement, le processus de mise en œuvre comprend ce qui suit:

a) la délivrance d'un mandat et d'un engagement, si nécessaire;

b) une analyse des écarts;

c) une adaptation personnalisée et un barème déterminés à partir des besoins organisationnels, de la culture, de la création de valeur et de sa préservation;

d) une évaluation des risques associés à la transition;

e) l'élaboration d'un plan d'activité

   — fixant des objectifs, des priorités et des mesures,

   — établissant l'étude de marché, y compris l'alignement sur les objectifs organisationnels, et

   — déterminant la portée, les responsabilités, le calendrier et les ressources;

f) l'identification du contexte de mise en œuvre, y compris la communication avec les parties prenantes.

3.3.3 Conception du cadre organisationnel

3.3.3.1 Il convient d'évaluer les modalités existantes du management du risque de l'organisme, en incluant le contexte et la culture.

a) Il est important de tenir compte de toutes les obligations légales, réglementaires ou commerciales, ainsi que des exigences de certification découlant des systèmes de management et des normes auxquels l'organisme a choisi d'adhérer. L'objectif de cette étape est de permettre une adaptation personnalisée et minutieuse de la conception du cadre organisationnel de management du risque et du plan de mise en œuvre, ainsi que de permettre leur alignement sur la structure, la culture et le système général de management de l'organisme.

b) Il est important d'étudier le processus utilisé pour gérer les risques et les aspects du cadre organisationnel de management du risque existant permettant la mise en pratique de ce processus.

c) Il convient de définir des critères de risque appropriés. Les critères de risque doivent être cohérents avec les objectifs de l'organisme et alignés sur son attitude face au risque. Si les objectifs changent, les critères de risque nécessitent d'être ajustés en conséquence. Il est important pour un management du risque efficace que les critères de risque soient élaborés de sorte à correspondre à l'attitude de l'organisme face au risque et à ses objectifs.

Pour la conception du nouveau cadre organisationnel, il convient d'évaluer de manière spécifique:

— les principes et les attributs, comme décrit dans l'ISO 31000;

— l'ancien cadre organisationnel, dont il convient en particulier de comparer les pratiques les plus récentes avec les exigences des paragraphes suivants de l'ISO 31000:2009:

   — 4.3.2 (politique de management du risque);

   — 4.3.3 (responsabilité);

   — 4.3.4 (intégration aux processus organisationnels);

   — 4.3.5 (ressources);

   — 4.3.6 et 4.3.7 (mécanismes de communication et de rapports internes et externes);

— le processus, pour lequel il convient de comparer les éléments des processus existants avec ceux de l'ISO 31000:2009, Article 5, ainsi que les principes sous-jacents qui motivent et déterminent la

raison d'être du processus avec les principes fixés dans l'ISO 31000:2009, Article 3 (par exemple si le processus influe réellement ou non sur la prise de décision à tous les niveaux):

— évaluer si le processus actuel fournit aux décisionnaires les informations sur le risque dont ils ont besoin pour prendre des décisions judicieuses et atteindre ou dépasser les objectifs;

— évaluer si les modalités existantes de management du risque traitent suffisamment des risques interdépendants et des risques survenant en des endroits multiples.

3.3.3.2 Il convient d'identifier les exigences de conception du cadre organisationnel.

En s'appuyant sur les évaluations décrites en 3.3.3.1, il convient que l'organisme détermine quels aspects de l'approche existante du management du risque:

a) peuvent être préservés à l'avenir (voire être étendus à d'autres types de prise de décision);

b) nécessitent des modifications ou des améliorations;

c) n'ajoutent plus de valeur et qu'il convient d'abandonner.

Il convient que l'organisme développe, documente et communique ses modalités de gestion du risque. Il convient que l'importance et le contenu des normes, des principes directeurs et des modèles de l'organisme liés au management du risque reflètent le contexte et la culture organisationnels.

Ces documents peuvent spécifier que:

— les risques sont gérés à tous les niveaux de l'organisme selon des modalités cohérentes;

— il existe différents niveaux de responsabilité de management du risque;

— les compétences et les devoirs de toutes les personnes assurant des responsabilités de management du risque sont clairement définis;

— les parties prenantes internes et externes sont impliquées, comme il convient, par le biais d'une communication et d'une concertation globales;

— les informations sur les risques et les résultats de toutes les applications du processus de management du risque sont enregistrés de manière cohérente et sûre, avec des droits de consultation appropriés.

Il convient également de prévoir des dispositions concernant la revue périodique des exigences, des outils, de la formation et des ressources organisationnels liés au management du risque, en cas de changements ultérieurs apportés à l'organisme et son contexte ou si la surveillance en continu et la revue identifient des faiblesses ou des inefficacités.

3.3.3.3 Il convient de définir la portée, les objectifs, les cibles, les ressources, les mesures de réussite et les critères de surveillance et de revue pour la phase de mise en œuvre.

3.3.3.4 Il convient de déterminer des mécanismes de communication et de rapport internes et externes.

3.3.4 Mise en œuvre du management du risque

Un plan de mise en œuvre détaillé est nécessaire pour garantir que les changements indispensables s'effectuent dans un ordre cohérent et que les ressources associées peuvent être fournies et utilisées. Il convient que le plan soit accompagné des ressources nécessaires à sa mise en œuvre et ceci peut requérir l'attribution de budgets spécifiques, dont il convient que la mise à disposition fasse partie du processus de planification.

Il convient que le plan lui-même soit soumis à une appréciation du risque conformément à l'ISO 31000:2009, 5.4, et que toute action de traitement du risque nécessaire soit mise en œuvre.

Il convient que le plan requière et permette que les progrès soient suivis et rapportés à la direction générale et à l'organe de surveillance; il convient également que soient prévues des dispositions concernant les revues périodiques du plan.

Il convient, par conséquent, que le plan:

— détaille les actions spécifiques à entreprendre, leur séquencement, les personnes devant les réaliser et le délai de réalisation; ces actions comprendront également les modifications à apporter aux normes et aux principes directeurs internes, des explications et des formations en vue de forger des aptitudes, ainsi que les ajustements à opérer au niveau des responsabilités;

— identifie les actions qui seront mises en œuvre dans le cadre d'actions plus larges associées à un développement organisationnel ou liées à celui-ci de toute autre manière (par exemple développement de documents de formation et engagement de formateurs);

— définit les responsabilités liées à l'implémentation;

— comporte un mécanisme de rapport des réalisations, des avancées et des problèmes;

— identifie et enregistre tout critère qui déclenchera une revue du plan.

La mise en œuvre peut prendre un certain temps pour être conclue et peut être réalisée en plusieurs étapes. Il convient d'adopter la pratique habituelle consistant à donner la priorité chaque fois que cela est possible aux changements ayant le plus gros impact sur la réalisation de l'objectif final. Cette mise en œuvre peut se produire à divers stades de la maturité et de la structure organisationnelles. Il peut également s'avérer plus efficace d'intégrer la mise en œuvre à d'autres programmes entraînant des changements.

3.3.5 Surveillance et revue

Il convient de suivre, d'analyser et de rapporter à la direction générale les progrès réalisés par rapport au plan, et ce en temps opportun (mensuellement, trimestriellement, etc.).

Il convient de valider périodiquement les rapports sur les progrès réalisés en fonction du plan et les performances en fonction des mesures dans un processus de revue objectif et impartial. Il convient que les revues prévoient un examen du cadre organisationnel, des processus, des risques eux-mêmes et des changements de l'environnement.

Il convient de procéder à une revue périodique de la stratégie de mise en œuvre, avec un mesurage des progrès, ainsi que de sa cohérence et des écarts constatés par rapport au plan de management du risque. Il peut également y avoir des revues lorsque les critères de revue définis dans le plan sont réunis.

Il convient d'évaluer la performance par rapport à l'efficacité du changement et à la gestion du risque, ainsi qu'en fonction des enseignements tirés et des opportunités d'amélioration.

Il convient de rapporter aux personnes responsables les conclusions significatives de la surveillance.

Les résultats de cette étape seront répercutés sur le contexte et les autres fonctions, de sorte à pouvoir identifier de nouveaux risques, découvrir des changements apportés aux risques existants et enregistrer l'état d'exécution du cadre organisationnel en vue d'améliorations (voir l'ISO 31000:2009, 4.6 et 5.7).

3.4 Amélioration continue

Il convient de procéder à une revue du cadre organisationnel et du processus de management du risque pour évaluer si leur conception est pertinente et si leur mise en œuvre ajoute de la valeur à l'organisme comme prévu. Si les résultats de la surveillance et de la revue montrent que des améliorations peuvent être apportées, il convient que celles-ci soient mises en œuvre dès que possible.

Dans les organismes ayant réalisé la transition vers l'ISO 31000, il convient de faire preuve d'une vigilance et d'un intérêt constant pour les opportunités d'amélioration. Il est également utile d'appliquer

les mêmes étapes que celles du processus de transition aux contrôles périodiques réalisés pour vérifier les éventuels écarts par rapport au processus.

Il existe divers éléments déclencheurs d'amélioration continue, notamment:

— la surveillance et la revue routinières du cadre organisationnel et du processus de management du risque, qui identifient les opportunités d'amélioration;

— l'apparition de nouvelles connaissances;

— un changement substantiel apporté aux contextes interne et externe de l'organisme.