NORME INTERNATIONALE

ISO 31000

Première édition
2009-11-15

Management du risque — Principes et lignes directrices

Risk management — Principles and guidelines

Numéro de référence
ISO 31000:2009(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

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 Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

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.

L'ISO 31000 a été élaborée par le groupe de travail du Bureau de gestion technique ISO sur le Management du risque.

Introduction

Les organismes de tous types et de toutes dimensions confrontés à des facteurs et des influences internes et externes ignorent si et quand ils vont atteindre leurs objectifs. L'incidence de cette incertitude sur l'atteinte des objectifs d'un organisme constitue le «risque».

Toutes les activités d'un organisme comprennent des risques. Les organismes gèrent le risque en l'identifiant, en l'analysant, et en évaluant ensuite la nécessité de le modifier par un traitement afin de satisfaire aux critères de risque. Tout au long de ce processus, ils communiquent et se concertent avec les parties prenantes, et surveillent et revoient le risque et les moyens de maîtrise qui modifient le risque afin de s'assurer qu'il n'est pas nécessaire de recourir à un traitement supplémentaire du risque. La présente Norme internationale décrit ce processus systématique et logique en détail.

Alors que tous les organismes gèrent des risques à différents niveaux, la présente Norme internationale fixe un certain nombre de principes qui doivent être appliqués pour rendre le management du risque efficace. La présente Norme internationale recommande que les organismes élaborent, mettent en œuvre et améliorent continuellement un cadre organisationnel dont le but est d'intégrer le processus de management du risque aux processus de gouvernance, de stratégie et de planification, de management, de rédaction des rapports, ainsi qu'aux politiques, aux valeurs et à la culture d'ensemble de l'organisme.

Le management du risque peut s'appliquer à l'ensemble de l'organisme, dans tous ses domaines et à tous ses niveaux, à tout moment, ainsi qu'à des fonctions, des projets et des activités particulières.

Même si la pratique du management du risque s'est développée au fil du temps et dans de nombreux secteurs pour répondre à différents besoins, l'adoption de processus cohérents dans un cadre organisationnel complet peut contribuer à garantir que le risque est géré de façon efficace, performante et cohérente au sein d'un organisme. L'approche générique décrite dans la présente Norme internationale fournit des principes et des lignes directrices pour gérer toute forme de risque de manière systématique, transparente et fiable, dans quelque domaine et quelque contexte que ce soit.

Chaque secteur ou application particulier du management du risque comporte des besoins, des publics, des perceptions et des critères qui lui sont propres. C'est pourquoi, l'un des points essentiels de la présente Norme internationale est d'intégrer «l'établissement du contexte» en tant qu'activité de départ du processus générique de management du risque. Établir le contexte va permettre d'appréhender les objectifs de l'organisme, l'environnement dans lequel il poursuit ces objectifs, les parties prenantes et la diversité des critères de risques, tous ces éléments devant contribuer à révéler et apprécier la nature et la complexité de ses risques.

La Figure 1 illustre les relations entre les principes de management du risque, le cadre organisationnel dans lequel il se présente et le processus de management du risque décrits dans la présente Norme internationale.

La mise en œuvre et le maintien du management du risque conformément à la présente Norme internationale permettent, par exemple, à un organisme

— d'accroître la vraisemblance d'atteindre les objectifs,

— 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 la rédaction des rapports obligatoires et volontaires,

— 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 moyens de maîtrise,

— 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, et

— d'améliorer la résilience organisationnelle.

La présente Norme internationale est destinée à répondre aux besoins d'une grande diversité de parties prenantes, dont

a) les personnes responsables de l'élaboration d'une politique de management du risque au sein de leur organisme,

b) les personnes chargées de s'assurer que ce risque est géré efficacement au sein de l'organisme dans son ensemble ou dans un domaine, une activité ou un projet spécifique,

c) les personnes chargées d'évaluer l'efficacité d'un organisme en matière de management du risque, et

d) les rédacteurs de normes, guides, procédures et bonnes pratiques qui, en totalité ou en partie, déterminent la manière dont le risque doit être géré dans le contexte spécifique de ces documents.

Les pratiques et processus de management en cours dans nombre d'organismes comportent des éléments de management du risque, et beaucoup d'organismes ont déjà adopté un processus formalisé de management du risque pour des types particuliers de risques ou de situations. Dans de tels cas, un organisme peut décider de réaliser une revue critique de ses pratiques et processus existants à la lumière de la présente Norme internationale.

Dans la présente Norme internationale les expressions «management du risque» et «gérer le risque» sont toutes deux utilisées. De façon générale, le «management du risque» se réfère à la structure (principe, cadre organisationnel et processus) permettant de gérer le risque avec efficacité, alors que «gérer le risque» se réfère à l'application de cette structure aux risques particuliers.

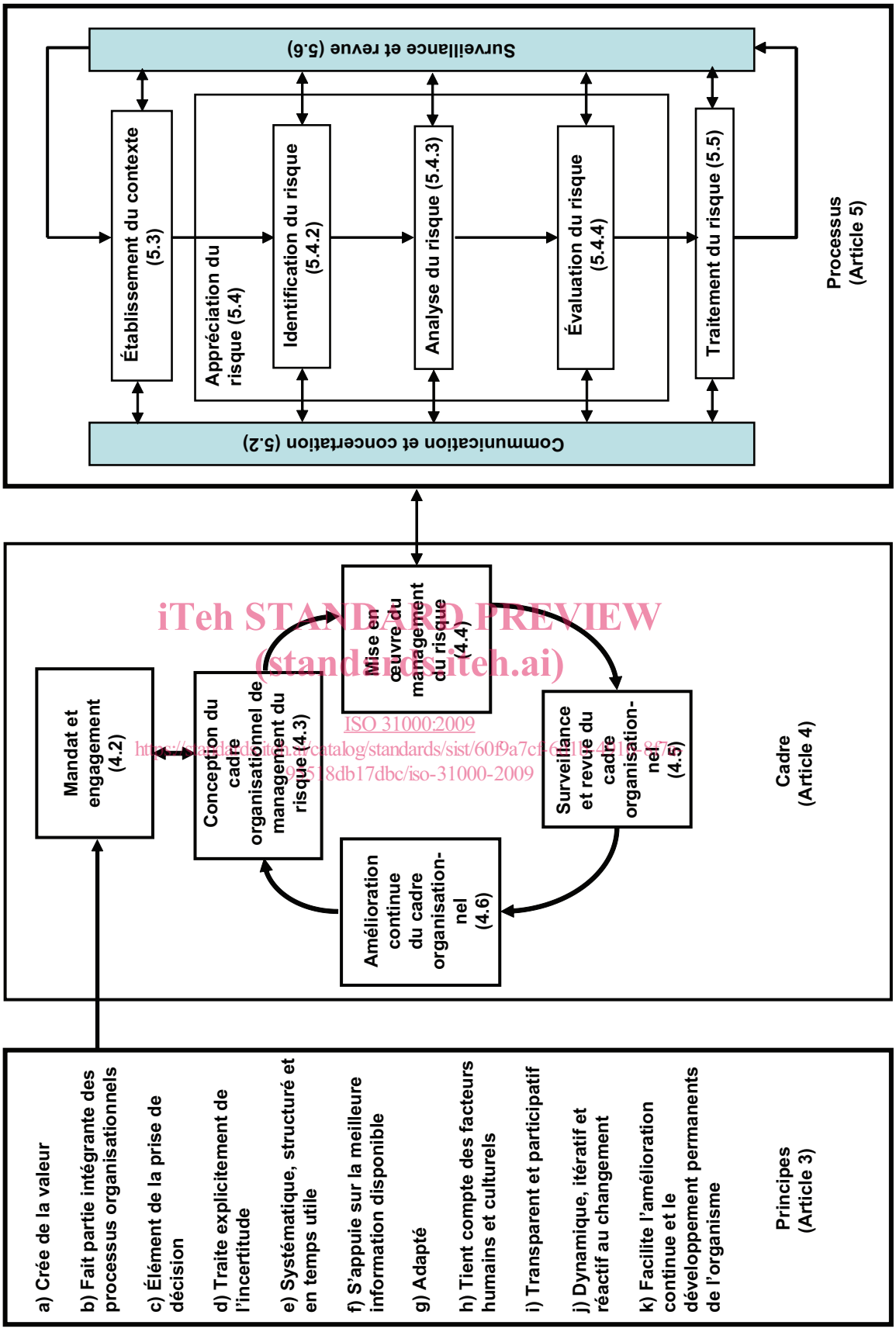

Figure 1 — Relations entre les principes, le cadre organisationnel et le processus de management du risque

Management du risque — Principes et lignes directrices

1 Domaine d'application

La présente Norme internationale fournit des principes et des lignes directrices générales sur le management du risque.

La présente Norme internationale peut être appliquée par tout public, toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu. Par conséquent, la présente Norme internationale n'est pas spécifique à une industrie ou un secteur donné.

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

La présente Norme internationale peut être appliquée tout au long de la vie d'un organisme et à une large gamme d'activités, dont les stratégies et les prises de décisions, les activités opérationnelles, les processus, les fonctions, les projets, les produits, les services et les actifs.

La présente Norme internationale peut s'appliquer à tout type de risque, quelle que soit sa nature, que ses conséquences soient positives ou négatives.

Bien que la présente Norme internationale fournisse des lignes directrices générales, elle ne vise pas à promouvoir l'uniformisation du management du risque au sein des organismes. La conception et la mise en œuvre des plans et des structures organisationnelles de management du risque devront tenir compte des divers besoins d'un organisme spécifique, de ses objectifs, son contexte, sa structure, son activité, ses processus, ses fonctions, ses projets, ses produits, ses services ou ses actifs particuliers, ainsi que de ses pratiques spécifiques.

Il est prévu que la présente Norme internationale serve à harmoniser les processus de management du risque dans les normes existantes et à venir. Elle offre une approche commune à l'établissement des normes traitant de risques et/ou secteurs spécifiques, sans toutefois remplacer ces normes.

La présente Norme internationale n'a pas vocation à servir de base à une certification.

2 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

2.1
risque
effet de l'incertitude sur l'atteinte des objectifs

NOTE 1 Un effet est un écart, positif et/ou négatif, par rapport à une attente.

NOTE 2 Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier).

NOTE 3 Un risque est souvent caractérisé en référence à des **événements** (2.17) et des **conséquences** (2.18) potentiels ou à une combinaison des deux.

NOTE 4 Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa **vraisemblance** (2.19).

NOTE 5 L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

[ISO Guide 73:2009, définition 1.1]

2.2
management du risque
activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du **risque** (2.1)

[ISO Guide 73:2009, définition 2.1]

2.3
cadre organisationnel de management du risque
ensemble d'éléments établissant les fondements et dispositions organisationnelles présidant à la conception, la mise en œuvre, la **surveillance** (2.28), la revue et l'amélioration continue du **management du risque** (2.2) dans tout l'organisme

NOTE 1 Les fondements incluent la politique, les objectifs, le mandat et l'engagement envers le management du **risque** (2.1).

NOTE 2 Les dispositions organisationnelles incluent les plans, les relations, les responsabilités, les ressources, les processus et les activités.

NOTE 3 Le cadre organisationnel du management du risque fait partie intégrante des politiques stratégiques et opérationnelles ainsi que des pratiques de l'ensemble de l'organisme.

[ISO Guide 73:2009, définition 2.1.1]

2.4
politique de management du risque
déclaration des intentions et des orientations générales d'un organisme en relation avec le **management du risque** (2.2)

[ISO Guide 73:2009, définition 2.1.2]

2.5
attitude face au risque
approche d'un organisme pour apprécier un **risque** (2.1) avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque

[ISO Guide 73:2009, définition 3.7.1.1]

2.6
plan de management du risque
programme inclus dans le **cadre organisationnel de management du risque** (2.3), spécifiant l'approche, les composantes du management et les ressources auxquelles doit avoir recours le management du **risque** (2.1)

NOTE 1 Les composantes du management incluent, par exemple, les procédures, les pratiques, l'attribution des responsabilités, le déroulement chronologique des activités.

NOTE 2 Le plan de management du risque peut être appliqué à un produit, un processus, un projet particulier, à une partie de l'organisme ou à l'organisme tout entier.

[ISO Guide 73:2009, définition 2.1.3]

2.7
propriétaire du risque
personne ou entité ayant la responsabilité du **risque** (2.1) et ayant autorité pour le gérer

[ISO Guide 73:2009, définition 3.5.1.5]

2.8
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** (2.28) et de revue des **risques** (2.1)

[ISO Guide 73:2009, définition 3.1]

2.9
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** (2.22) pour la **politique de management du risque** (2.4)

[ISO Guide 73:2009, définition 3.3.1]

2.10
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses objectifs

NOTE Le contexte externe peut inclure

— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,

— les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme, et

— les relations avec les **parties prenantes** (2.13) externes, leurs perceptions et leurs valeurs.

[ISO Guide 73:2009, définition 3.3.1.1]

2.11
contexte interne
environnement interne dans lequel l'organisme cherche à atteindre ses objectifs

NOTE Le contexte interne peut inclure

— la gouvernance, l'organisation, les rôles et responsabilités,

— les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers,

— les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies),

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels),

— les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs,

— la culture de l'organisme,

— les normes, lignes directrices et modèles adoptés par l'organisme, et

— la forme et l'étendue des relations contractuelles.

[ISO Guide 73:2009, définition 3.3.1.2]

2.12
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** (2.13) et autres parties, concernant le management du **risque** (2.1)

NOTE 1 Ces informations peuvent concerner l'existence, la nature, la forme, la **vraisemblance** (2.19), l'importance, l'évaluation, l'acceptabilité et le traitement du management du risque.

NOTE 2 La concertation est un processus de communication argumentée à double sens entre un organisme et ses parties prenantes sur une question donnée avant de prendre une décision ou de déterminer une orientation concernant ladite question. La concertation est

— un processus dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir, et

— une contribution à une prise de décision, et non une prise de décision conjointe.

[ISO Guide 73:2009, définition 3.2.1]

2.13
partie prenante
personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

NOTE Un décideur peut être une partie prenante.

[ISO Guide 73:2009, définition 3.2.1.1]

2.14
appréciation du risque
ensemble du processus d'**identification des risques** (2.15), d'**analyse du risque** (2.21) et d'**évaluation du risque** (2.24)

[ISO Guide 73:2009, définition 3.4.1]

2.15
identification des risques
processus de recherche, de reconnaissance et de description des **risques** (2.1)

NOTE 1 L'identification des risques comprend l'identification des **sources de risque** (2.16), des **événements** (2.17), de leurs causes et de leurs **conséquences** (2.18) potentielles.

NOTE 2 L'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des **parties prenantes** (2.13).

[ISO Guide 73:2009, définition 3.5.1]

2.16
source de risque
tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un **risque** (2.1)

NOTE Une source de risque peut être tangible ou intangible.

[ISO Guide 73:2009, définition 3.5.1.2]

2.17
événement
occurrence ou changement d'un ensemble particulier de circonstances

NOTE 1 Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.