

ICS: 03.100.01

***norme belge
enregistrée***

NBN ISO 31000

1e éd., juin 2014

Indice de classement: X 50

Management du risque - Principes et lignes directrices (ISO 31000:2009)

Risicomanagement - Principes en richtlijnen (ISO 31000:2009)

Risk management - Principles and guidelines (ISO 31000:2009)

Autorisation de publication: 20 juin 2014

La présente norme ISO 31000:2009 a le statut d'une norme belge.

La présente norme existe en deux versions officielles (anglais, français).



Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique

Tél: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be

Banque 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB TVA BE0880857592

ICS: 03.100.01

Geregistreeerde Belgische norm

NBN ISO 31000

1e uitg., juni 2014

Normklasse: X 50

Risicomanagement - Principes en richtlijnen (ISO 31000:2009)

Management du risque - Principes et lignes directrices (ISO 31000:2009)

Risk management - Principles and guidelines (ISO 31000:2009)

Toelating tot publicatie: 20 juni 2014

Deze norm ISO 31000:2009 heeft de status van een Belgische norm.

Deze norm bestaat in twee officiële versies (Engels, Frans).



Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België

Tel: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be

Bank 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB BTW BE0880857592

NBN ISO 31000 (2014)

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 2009

PDF – Exonération de responsabilité

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO 2009

Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

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 | iv |
| Introduction..... | v |
| 1 Domaine d'application | 1 |
| 2 Termes et définitions | 1 |
| 3 Principes..... | 7 |
| 4 Cadre organisationnel..... | 8 |
| 4.1 Généralités | 8 |
| 4.2 Mandat et engagement..... | 9 |
| 4.3 Conception du cadre organisationnel de management du risque | 10 |
| 4.3.1 Compréhension de l'organisme et de son contexte | 10 |
| 4.3.2 Établissement de la politique de management du risque | 10 |
| 4.3.3 Responsabilité | 11 |
| 4.3.4 Intégration aux processus organisationnels..... | 11 |
| 4.3.5 Ressources | 11 |
| 4.3.6 Établissement de mécanismes de communication et de rapports internes | 12 |
| 4.3.7 Établissement de mécanismes de communication et de rapports externes | 12 |
| 4.4 Mise en œuvre du management du risque | 12 |
| 4.4.1 Mise en œuvre du cadre organisationnel de management du risque | 12 |
| 4.4.2 Mise en œuvre du processus de management du risque | 13 |
| 4.5 Surveillance et revue du cadre organisationnel | 13 |
| 4.6 Amélioration continue du cadre organisationnel | 13 |
| 5 Processus | 13 |
| 5.1 Généralités | 13 |
| 5.2 Communication et concertation | 14 |
| 5.3 Établissement du contexte | 15 |
| 5.3.1 Généralités | 15 |
| 5.3.2 Établissement du contexte externe | 15 |
| 5.3.3 Établissement du contexte interne..... | 15 |
| 5.3.4 Établissement du contexte du processus de management du risque | 16 |
| 5.3.5 Définition des critères de risque..... | 17 |
| 5.4 Appréciation du risque | 17 |
| 5.4.1 Généralités | 17 |
| 5.4.2 Identification du risque | 17 |
| 5.4.3 Analyse du risque..... | 18 |
| 5.4.4 Évaluation du risque | 18 |
| 5.5 Traitement du risque | 19 |
| 5.5.1 Généralités | 19 |
| 5.5.2 Sélection des options de traitement du risque | 19 |
| 5.5.3 Élaboration et mise en œuvre des plans de traitement du risque | 20 |
| 5.6 Surveillance et revue..... | 20 |
| 5.7 Enregistrement du processus de management du risque..... | 21 |
| Annexe A (informative) Attributs d'un management du risque élevé..... | 22 |
| Bibliographie..... | 24 |

ISO 31000:2009(F)**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,

ISO 31000:2009(F)

- 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.

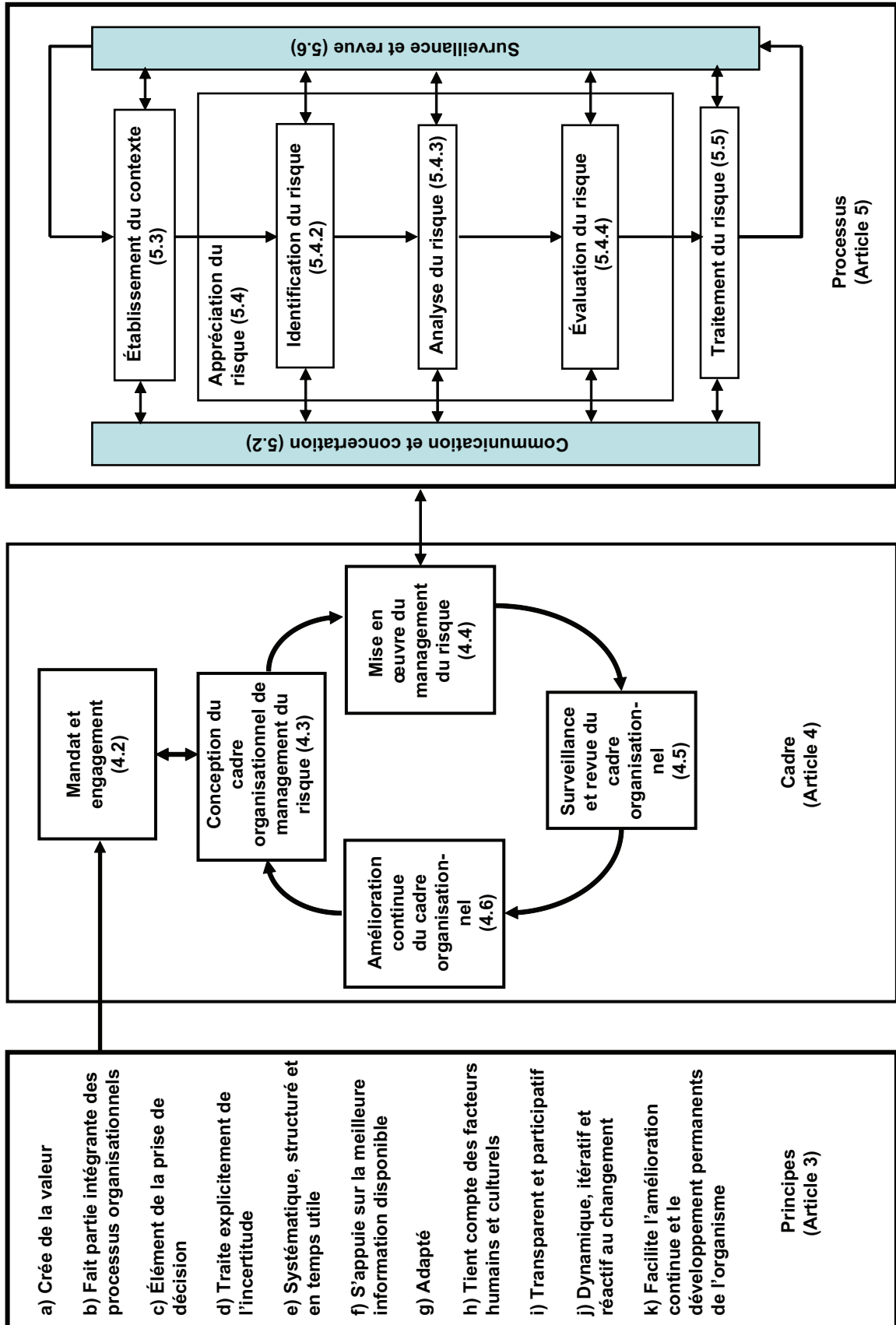


Figure 1 — Relations entre les principes, le cadre organisationnel et le processus de management du risque

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.