

ICS: 03.100.01

***norme belge
enregistrée***

NBN ISO/TR 31004

1e éd., juin 2014

Indice de classement: X 50

Management du risque - Lignes directrices pour l'implémentation de l'ISO 31000 (ISO/TR 31004:2013)

Risicomanagement - Richtlijn voor het toepassen van ISO 31000 (ISO/TR 31004:2013)

Risk management - Guidance for the implementation of ISO 31000 (ISO/TR 31004:2013)

Autorisation de publication: 20 juin 2014

L'ISO/TR 31004:2013 est enregistrée en tant que document belge

Ce document 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/TR 31004

1e uitg., juni 2014

Normklasse: X 50

Risicomanagement - Richtlijn voor het toepassen van ISO 31000 (ISO/TR 31004:2013)

Management du risque - Lignes directrices pour l'implémentation de l'ISO 31000 (ISO/TR 31004:2013)

Risk management - Guidance for the implementation of ISO 31000 (ISO/TR 31004:2013)

Toelating tot publicatie: 20 juni 2014

De ISO/TR 31004:2013 is geregistreerd als Belgische document.

Dit document 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/TR 31004 (2014)

RAPPORT TECHNIQUE

ISO/TR 31004

Première édition
2013-10-15

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

Risk management — Guidance for the implementation of ISO 31000



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

© ISO 2013



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2013

Droits de reproduction réservés. Sauf indication contraire, 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, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au 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

Version française parue en 2014

Publié en Suisse

Sommaire

	Page
Avant-propos	iv
Introduction	v
1 Domaine d'application	1
2 Références normatives	1
3 Mise en œuvre de l'ISO 31000	1
3.1 Généralités.....	1
3.2 Comment mettre en œuvre l'ISO 31000.....	2
3.3 Intégration de l'ISO 31000 aux processus de management de l'organisme.....	3
3.4 Amélioration continue.....	6
Annexe A (informative) Concepts et principes sous-jacents	8
Annexe B (informative) Application des principes de l'ISO 31000	11
Annexe C (informative) Comment exprimer mandat et engagement	22
Annexe D (informative) Surveillance et revue	26
Annexe E (informative) Intégration du management du risque à un système de management	36
Bibliographie	39

ISO/TR 31004:2013(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 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'implémentation 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.