

ISO 31000:2018
NBN ISO 31000:2018

 **NBN**



Management du risque - Lignes directrices (ISO 31000:2018)

Valable à partir de 28-02-2018

Remplace NBN ISO/DIS 31000:2017, NBN ISO 31000:2014 et NBN ISO 31000 NL:2014

ICS: 03.100.01

**NORME
INTERNATIONALE**

**ISO
31000**

Deuxième édition
2018-02

**Management du risque — Lignes
directrices**

Risk management — Guidelines



Numéro de référence
ISO 31000:2018(F)

ISO 31000:2018(F)**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO 2018

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en oeuvre, 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, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée 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 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Tél.: +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 Références normatives	1
3 Termes et définitions	1
4 Principes	2
5 Cadre organisationnel	4
5.1 Généralités.....	4
5.2 Leadership et engagement.....	5
5.3 Intégration.....	5
5.4 Conception.....	6
5.4.1 Compréhension de l'organisme et de son contexte.....	6
5.4.2 Définir clairement l'engagement en matière de management du risque.....	6
5.4.3 Attribution des rôles, pouvoirs et responsabilités au sein de l'organisme.....	7
5.4.4 Affectation des ressources.....	7
5.4.5 Établissement d'une communication et d'une concertation.....	7
5.5 Mise en œuvre.....	8
5.6 Évaluation.....	8
5.7 Amélioration.....	8
5.7.1 Adaptation.....	8
5.7.2 Amélioration continue.....	8
6 Processus	8
6.1 Généralités.....	8
6.2 Communication et consultation.....	9
6.3 Périmètre d'application, contexte et critères.....	10
6.3.1 Généralités.....	10
6.3.2 Définition du domaine d'application.....	10
6.3.3 Contexte interne et externe.....	10
6.3.4 Définition des critères de risque.....	11
6.4 Appréciation du risque.....	11
6.4.1 Généralités.....	11
6.4.2 Identification du risque.....	11
6.4.3 Analyse du risque.....	12
6.4.4 Évaluation du risque.....	13
6.5 Traitement du risque.....	13
6.5.1 Généralités.....	13
6.5.2 Sélection des options de traitement du risque.....	13
6.5.3 Élaboration et mise en œuvre des plans de traitement du risque.....	14
6.6 Suivi et revue.....	14
6.7 Enregistrement et élaboration de rapports.....	15
Bibliographie	16

ISO 31000:2018(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 (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, 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/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée 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 dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/TC 262, *Management du risque*.

Cette deuxième édition annule et remplace la première édition (ISO 31000:2009), qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

- revue des principes de management du risque, qui sont les critères clés de sa réussite;
- mise en exergue du leadership de la direction et de l'intégration du management du risque, en commençant par la gouvernance de l'organisme;
- importance accrue accordée à la nature itérative du management du risque, en notant que de nouvelles expériences, connaissances et analyses peuvent conduire à une révision des éléments, actions et moyens de maîtrise du processus à chacune de ses étapes;
- simplification du contenu en se concentrant davantage sur le maintien d'un modèle de système ouvert pour s'adapter à de multiples besoins et contextes.

Introduction

Le présent document s'adresse aux personnes qui, au sein des organismes, créent de la valeur et la préservent par le management du risque, la prise de décisions, la définition et l'atteinte d'objectifs et l'amélioration de la performance.

Les organismes de tous types et de toutes tailles sont confrontés à des facteurs et des influences internes et externes qui rendent l'atteinte de leurs objectifs incertaine.

Le management du risque est une activité itérative qui aide les organismes à développer une stratégie, atteindre des objectifs et prendre des décisions éclairées.

Le management du risque fait partie intégrante de la gouvernance et du leadership et a une importance fondamentale dans la façon dont l'organisme est géré à tous les niveaux. Il contribue à l'amélioration des systèmes de management.

Le management du risque est intégré à toutes les activités d'un organisme et inclut l'interaction avec les parties prenantes.

Le management du risque prend en considération le contexte interne et externe de l'organisme, y compris le comportement humain et les facteurs culturels.

Le management du risque est fondé sur les principes, le cadre organisationnel et le processus décrits dans le présent document, tel qu'illustré à la [Figure 1](#). Ces éléments peuvent déjà exister, en totalité ou en partie, au sein de l'organisme; toutefois, ils peuvent nécessiter une adaptation ou une amélioration afin que le management du risque soit efficient, efficace et cohérent.

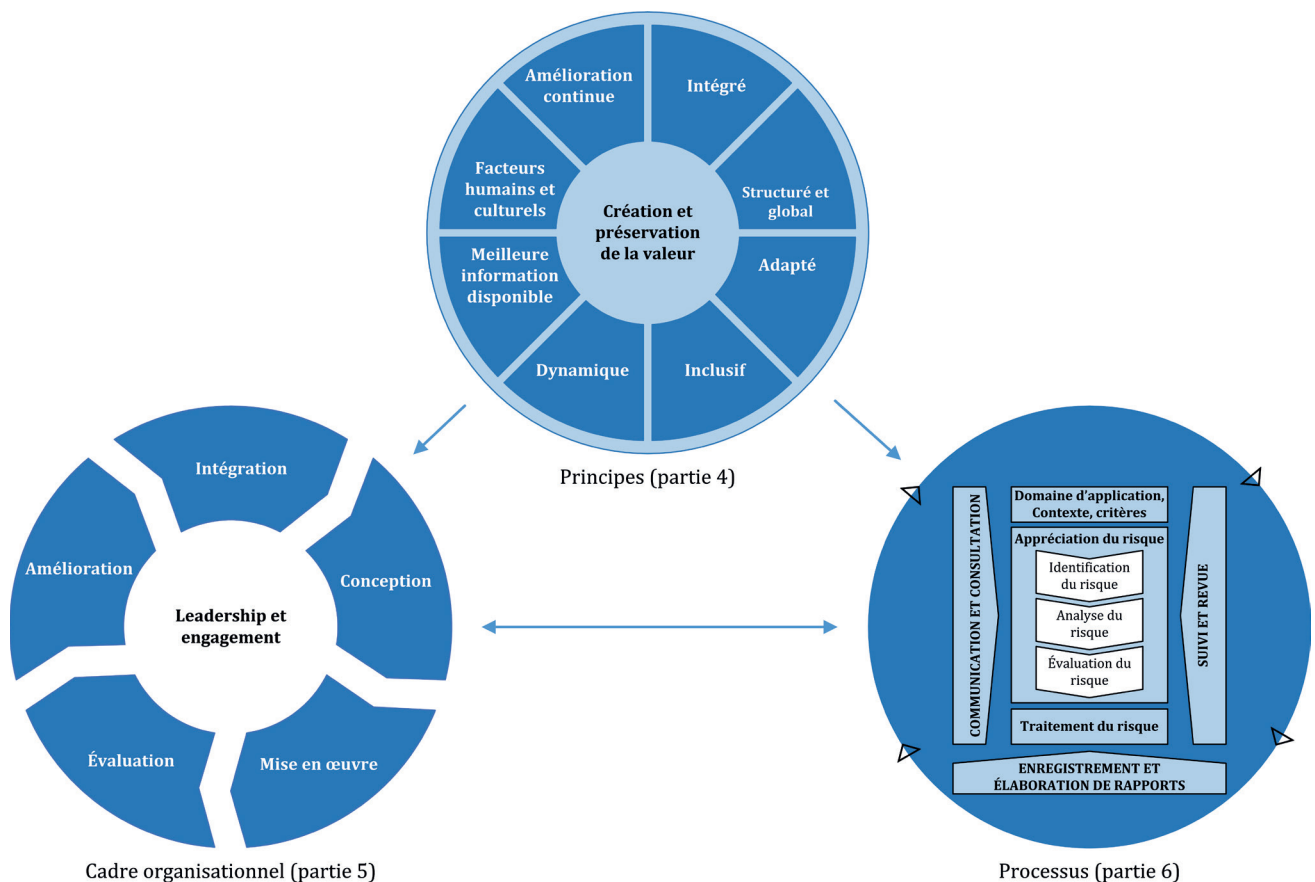


Figure 1 — Principes, cadre organisationnel et processus

Management du risque — Lignes directrices

1 Domaine d'application

Le présent document fournit des lignes directrices concernant le management du risque auquel sont confrontés les organismes. L'application de ces lignes directrices peut être adaptée à tout organisme et à son contexte.

Le présent document fournit une approche générique permettant de gérer toute forme de risque et n'est pas spécifique à une industrie ou un secteur.

Le présent document peut être utilisé tout au long de la vie de l'organisme et peut être appliqué à toute activité, y compris la prise de décisions à tous les niveaux.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- ISO Online browsing platform: disponible à l'adresse <https://www.iso.org/obp>
- IEC Electropedia: disponible à l'adresse <https://www.electropedia.org/>

3.1

risque

effet de l'incertitude sur les objectifs

Note 1 à l'article: Un effet est un écart par rapport à un attendu. Il peut être positif, négatif ou les deux à la fois, et traiter, créer ou entraîner des opportunités et des menaces.

Note 2 à l'article: Les objectifs peuvent avoir différents aspects, être de catégories différentes, et peuvent concerner différents niveaux.

Note 3 à l'article: Un risque est généralement exprimé en termes de *sources de risque* (3.4), *événements* (3.5) potentiels avec leurs *conséquences* (3.6) et leur *vraisemblance* (3.7).

3.2

management du risque

activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du *risque* (3.1)

3.3

partie prenante

personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir affecté par une décision ou une activité

Note 1 à l'article: Le terme «partie intéressée» peut être utilisé comme alternative à «partie prenante».

3.4

source de risque

tout élément qui, seul ou combiné à d'autres, est susceptible d'engendrer un *risque* (3.1)