NORME INTERNATIONALE

ISO 31000

Deuxième édition
2018-02

Management du risque — Lignes directrices

Risk management — Guidelines

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

Numéro de référence
ISO 31000:2018(F)

© ISO 2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-7ab50e5912da/iso-31000-2018

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-5e9b-4d1-b678-1d56c39129d/iso-31000-2018

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.

 © ISO 2018 – Tous droits réservés

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1e2e391239d/iso-31000-2018

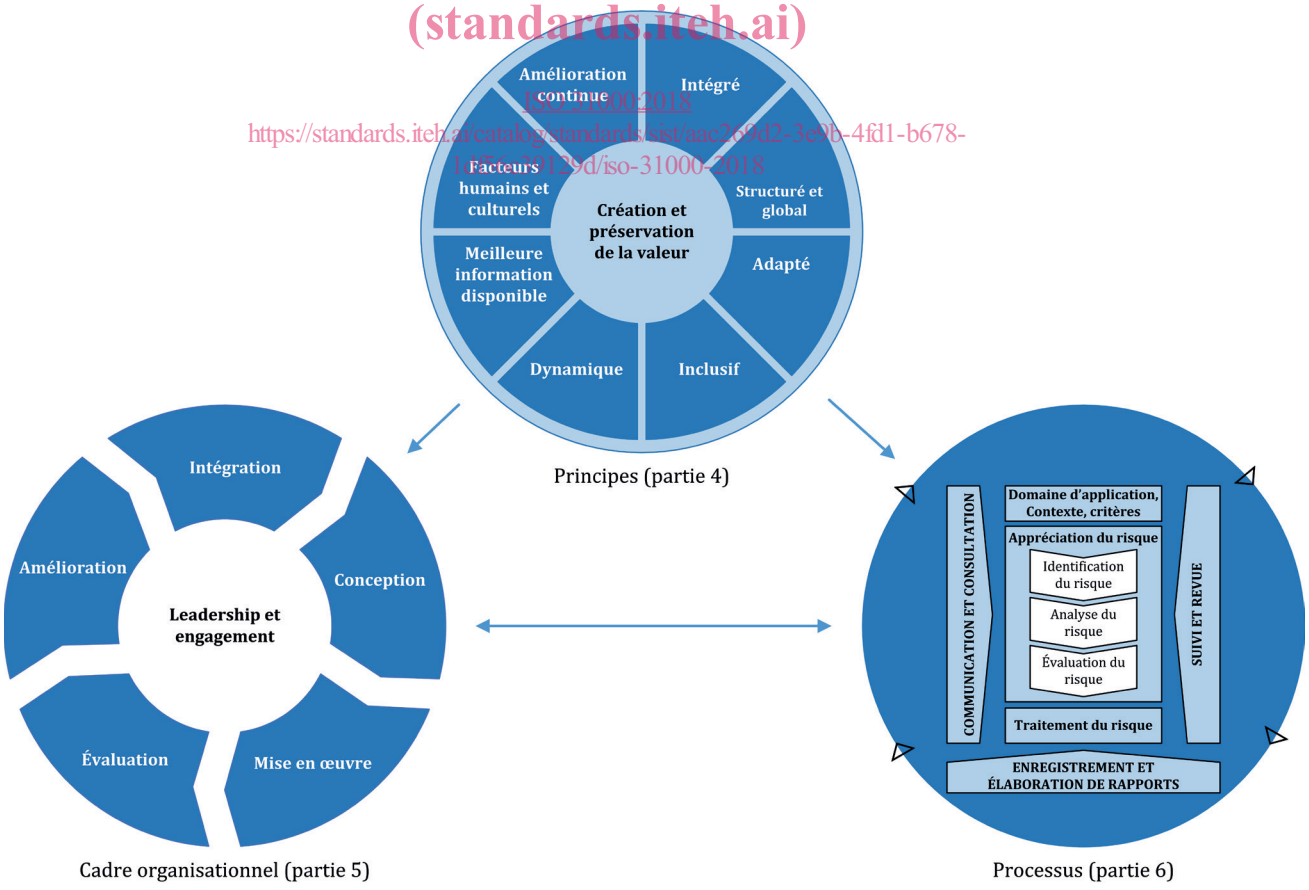


Figure 1 — Principes, cadre organisationnel et processus

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4f11-b678-1df56c39129d/iso-31000-2018

— 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)

© ISO 2018 – Tous droits réservés

3.5
événement
occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article: Un événement peut être unique ou se reproduire et peut avoir plusieurs causes et plusieurs *conséquences* (3.6).

Note 2 à l'article: Un événement peut être quelque chose qui est attendu, mais qui ne se produit pas, ou quelque chose auquel on ne s'attend pas, mais qui se produit.

Note 3 à l'article: Un événement peut être une source de risque.

3.6
conséquence
effet d'un *événement* (3.5) affectant les objectifs

Note 1 à l'article: Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs, directs ou indirects, sur l'atteinte des objectifs.

Note 2 à l'article: Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 3 à l'article: Toute conséquence peut déclencher des effets en cascade et cumulatifs.

3.7
vraisemblance
possibilité que quelque chose se produise

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Note 1 à l'article: Dans la terminologie du *management du risque* (3.2), le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e96-41d1-b678-1d36c39129d/iso-31000-2018

Note 2 à l'article: Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

3.8
moyen de maîtrise
action qui maintient et/ou modifie un *risque* (3.1)

Note 1 à l'article: Un moyen de maîtrise du risque inclut, sans toutefois s'y limiter, n'importe quels processus, politique, dispositif, pratique ou autres conditions et/ou actions qui maintiennent et/ou modifient un risque.

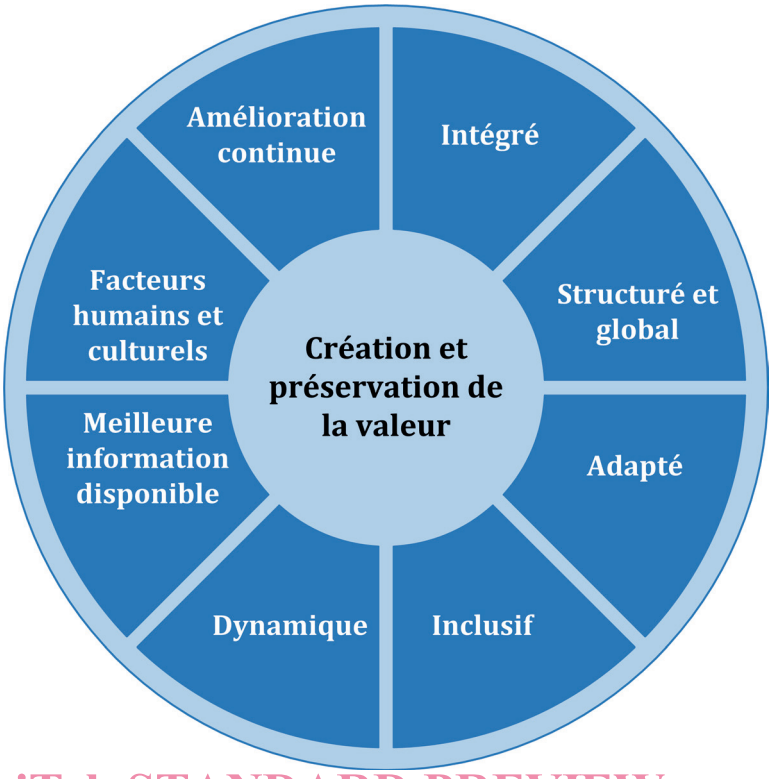
Note 2 à l'article: Un moyen de maîtrise du risque n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

4 Principes

La finalité du management du risque est la création et la préservation de la valeur. Il améliore la performance, favorise l'innovation et contribue à l'atteinte des objectifs.

Les principes rappelés à la Figure 2 fournissent les grands axes relatifs aux caractéristiques d'un management du risque efficace et efficient, en communiquant sa valeur et en expliquant son intention et sa finalité. Les principes sont le fondement du management du risque et il convient de les prendre en considération lors de l'établissement du cadre organisationnel et des processus de management du risque de l'organisme. Il convient que ces principes permettent à un organisme de gérer les effets de l'incertitude sur ses objectifs.

 © ISO 2018 – Tous droits réservés



iTeh STANDARD PREVIEW
(standards.iteh.ai)

Figure 2 — Principes

Un management du risque efficace nécessite les éléments de la Figure 2 et peut être expliqué plus en détail comme suit:

ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

a) Intégré

Le management du risque est intégré à toutes les activités de l'organisme.

b) Structuré et global

Une approche structurée et globale du management du risque contribue à la cohérence de résultats qui peuvent être comparés.

c) Adapté

Le cadre organisationnel et le processus de management du risque sont adaptés et proportionnés au contexte externe et interne de l'organisme aussi bien qu'à ses objectifs.

d) Inclusif

L'implication appropriée et au moment opportun des parties prenantes permet de prendre en compte leurs connaissances, leurs opinions et leur perception. Ceci conduit à un management du risque mieux éclairé et plus pertinent.

e) Dynamique

Des risques peuvent surgir, être modifiés ou disparaître lorsque le contexte externe et interne d'un organisme change. Le management du risque anticipe, détecte, reconnaît et réagit à ces changements et événements en temps voulu et de manière appropriée.

f) Meilleure information disponible

Les données d'entrée du management du risque sont fondées sur des informations historiques et actuelles ainsi que sur les attentes futures. Le management du risque tient compte explicitement

© ISO 2018 – Tous droits réservés

de toutes limites et incertitudes associées à ces informations et attentes. Il convient que les informations soient disponibles à temps, claires et accessibles aux parties prenantes pertinentes.

g) Facteurs humains et culturels

Le comportement humain et la culture influent de manière significative sur tous les aspects du management du risque à chaque niveau et à chaque étape.

h) Amélioration continue

Le management du risque est amélioré en continu par l'apprentissage et l'expérience.

5 Cadre organisationnel

5.1 Généralités

La finalité du cadre organisationnel de management du risque est d'aider l'organisme à intégrer le management du risque dans les activités et les fonctions significatives. L'efficacité du management du risque va dépendre de son intégration dans la gouvernance de l'organisme, y compris la prise de décisions. Cela nécessite un soutien et une implication des parties prenantes, en particulier de la direction.

Le développement du cadre organisationnel englobe l'intégration, la conception, la mise en œuvre, l'évaluation et l'amélioration du management du risque au sein de l'organisme. La Figure 3 illustre les composantes d'un cadre organisationnel.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 31000:2018
https://standards.iteh.ai/catalog/standards/sist/aac269d2-3e9b-4fd1-b678-1df56c39129d/iso-31000-2018

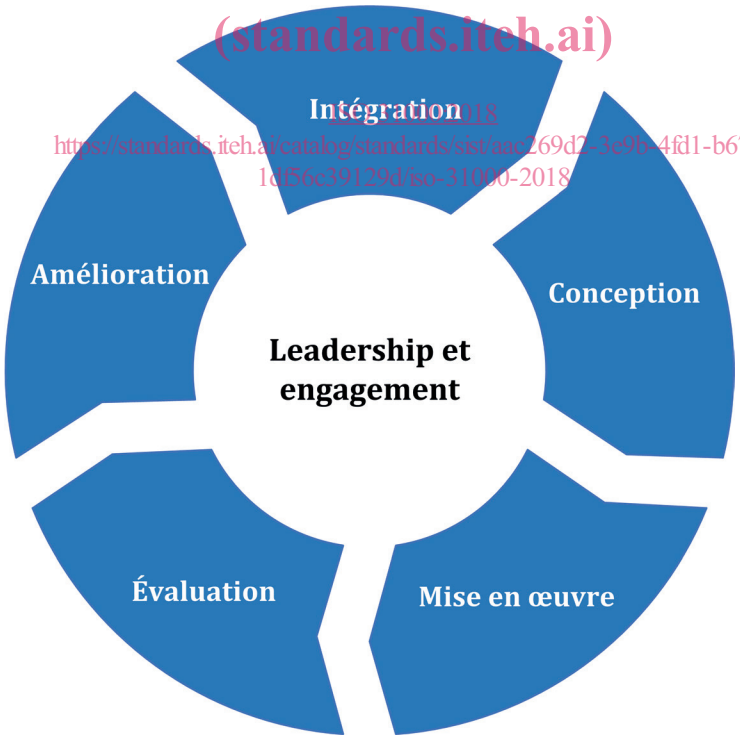


Figure 3 — Cadre organisationnel

Il convient que l'organisme évalue ses pratiques et processus existants de management du risque, identifie les lacunes et les comble avec le cadre organisationnel.

Il convient que les composantes du cadre organisationnel et la manière dont elles s'articulent soient adaptées aux besoins de l'organisme.

© ISO 2018 – Tous droits réservés

5.2 Leadership et engagement

Il convient que la direction et les organes de surveillance, le cas échéant, s'assurent que le management du risque est intégré dans toutes les activités de l'organisme et démontrent leur leadership et leur engagement en:

— adaptant et mettant en place toutes les composantes du cadre organisationnel;

— diffusant une déclaration ou une politique qui énonce une approche, un plan ou une ligne de conduite en matière de management du risque;

— s'assurant que les ressources nécessaires sont allouées au management du risque;

— attribuant l'autorité et la responsabilité aux niveaux appropriés de l'organisme.

Ceci aidera l'organisme à:

— aligner le management du risque sur sa stratégie, ses objectifs et sa culture;

— reconnaître et prendre en charge toutes les obligations ainsi que ses engagements volontaires;

— établir le niveau et le type de risque pouvant ou non être pris, afin de servir de guide à la mise en place de critères de risque, en s'assurant qu'ils sont communiqués à l'organisme et à ses parties prenantes;

— communiquer sur la valeur d'un management du risque pour l'organisme et ses parties prenantes;

— promouvoir un suivi systématique des risques;

— s'assurer que le cadre organisationnel de management du risque reste approprié au contexte de l'organisme.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 31000:2018

La direction est responsable du management du risque alors que les organes de surveillance sont responsables de la supervision du management du risque. Les organes de surveillance sont souvent censés ou tenus de:

— s'assurer que les risques sont pris en compte de manière adéquate lors de l'établissement des objectifs de l'organisme;

— comprendre les risques auxquels l'organisme s'expose dans la poursuite de ses objectifs;

— s'assurer que des systèmes permettant de gérer ces risques sont mis en œuvre et fonctionnent efficacement;

— s'assurer que ces risques sont adaptés au contexte des objectifs de l'organisme;

— s'assurer que les informations relatives à ces risques et à leur management sont communiquées de façon appropriée.

5.3 Intégration

L'intégration du management du risque s'appuie sur la compréhension des structures et du contexte de l'organisme. Les structures diffèrent selon la finalité, les objectifs et la complexité de l'organisme. Le risque est géré dans chaque partie de la structure de l'organisme. Chacun au sein d'un organisme a une responsabilité en matière de management du risque.

La gouvernance guide l'évolution de l'organisme, de ses relations externes et internes et des règles, processus et pratiques nécessaires pour atteindre sa finalité. Les structures de management traduisent l'orientation de la gouvernance en stratégie et objectifs associés requis pour atteindre les niveaux souhaités de performance durable et de viabilité à long terme. La détermination de la responsabilité du management du risque et des rôles de suivi au sein d'un organisme fait partie intégrante de la gouvernance de l'organisme.

© ISO 2018 – Tous droits réservés