ACCORDS INTERNATIONAUX D'ATELIER

ISO 31

Première édition
2020-03

Management du risque — Lignes directices pour l'utilisation de l'ISO 31000 dans les systèmes de management

Risk management — Guidelines on using ISO 31000 in management systems

Numéro de référence
IWA 31:2020(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
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

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 www.iso.org/avant-propos.

L'Accord international d'atelier IWA 31 a été adopté lors d'un atelier virtuel organisé par la BSI via Zoom en décembre 2019.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Introduction

Un nombre croissant d'organismes, de tous types et de toutes tailles, utilisent des systèmes de management fondés sur une norme de système de management (NSM) de l'ISO et de l'IEC[1]. De nouvelles NSM ISO et IEC continuent d'être élaborées pour traiter des aspects spécifiques des activités, produits ou services d'un organisme. Les Directives ISO/IEC, Partie 1, spécifie la structure-cadre des NSM. Cette structure générique spécifie un texte de base identique et des termes et définitions de base communs pour toutes les NSM ISO et IEC. Un organisme peut intégrer les exigences ou les recommandations de différentes NSM dans son système de management. La structure unifiée des NSM peut permettre aux utilisateurs construire plus facilement un système de management intégré (SMI), plutôt que de se retrouver avec un système de management fragmenté. Toutes ces NSM emploient le concept d'approche fondée sur le management du risque, d'approche fondée sur le risque ou d'approche risque (selon la terminologie utilisée dans le système de management en question), qui est au cœur de tout système de management. Le principal avantage en est l'application holistique de systèmes interreliés. L'ISO 31000:2018 peut être utilisée pour développer ou améliorer davantage un SMI grâce à ses recommandations sur la manière de déterminer les risques qu'il est nécessaire de prendre en compte pour donner l'assurance que le système de management peut atteindre les résultats escomptés, renforcer les effets désirés, prévenir ou réduire les effets non désirés et permettre une amélioration continue.

L'ISO 31000 représente les meilleures pratiques internationales en matière de management du risque. Celles-ci sont largement acceptées, génériques et adaptées au management de tout type de risque. Intégrer le management du risque dans son ou ses systèmes de management en utilisant l'ISO 31000 apporte de nombreux avantages à un organisme, qu'il s'agisse de traiter uniquement les effets négatifs ou d'inclure les effets positifs. La finalité du management du risque, telle que décrite dans l'ISO 31000, est la création et la préservation de la valeur. Il contribue à améliorer les décisions des propriétaires de risques ou de processus et renforce le fonctionnement des processus et de toutes les autres activités de l'organisme, y compris d'ordre stratégique et opérationnel. Cela peut conduire à de meilleurs résultats, à une plus grande qualité des éléments de sortie, à des erreurs moins coûteuses et à la gestion de la responsabilité.

L'intégration du management du risque conformément à l'ISO 31000 permet de créer de la valeur et de la préserver au sein des organismes en favorisant l'atteinte des objectifs et en rendant l'organisme plus résilient face aux effets adverses. L'appréciation des risques permet leur traitement approprié et établit une base pour accroître l'efficacité du système de management de l'organisme, obtenir de meilleurs résultats et prévenir les conséquences négatives. Cependant, l'intégration du management du risque dans un système de management peut poser des difficultés, qu'il est possible de réduire en suivant les recommandations du présent document.

1) Une liste des NSM ISO et IEC est disponible à l'adresse suivante: https://www.iso.org/management-system-standards-list.html.

Management du risque — Lignes directices pour l'utilisation de l'ISO 31000 dans les systèmes de management

1 Domaine d'application

Le présent document donne des lignes directrices pour l'intégration et l'utilisation de l'ISO 31000 dans les organismes ayant mis en œuvre une ou plusieurs normes de systèmes de management (NSM) de l'ISO et de l'IEC, ou ayant décidé d'entreprendre un projet mettant en œuvre une ou plusieurs NSM incorporant l'ISO 31000. Le présent document explique comment les articles de l'ISO 31000 se rapportent à la structure-cadre des NSM.

Le présent document ne fournit pas de recommandations pour la mise en œuvre d'un système de management en général. Il ne spécifie pas les exigences d'une NSM. Il ne fournit pas de résumé de l'ISO 31000; cependant, comme expliqué ci-dessus, il fournit les grandes lignes permettant de comprendre l'ISO 31000. L'utilisation du présent document ne dispense pas de la nécessité d'utiliser d'autres normes pour traiter des aspects spécifiques du risque.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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 31000:2018, *Management du risque — Lignes directrices*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO 31000:2018 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 http://www.electropedia.org/

4 Utilisation du terme «risque» dans l'ISO 31000 et les autres normes

Il convient d'appréhender la terminologie dans le contexte dans lequel elle est appliquée. Concernant le management du risque d'un organisme, l'ISO 31000:2018, 3.1, définit le «risque» comme l'«effet de l'incertitude sur les objectifs». Certaines normes ne font pas référence aux objectifs, mais le texte indique généralement qu'il est nécessaire de prendre en compte les risques afin de donner l'assurance que le système de management peut atteindre les résultats escomptés. Un objectif peut être exprimé sous la forme d'un résultat ou d'un effet escompté.

Le cadre organisationnel et le processus de management du risque de l'ISO 31000 sont ajustés et proportionnés au contexte externe et interne de l'organisme ainsi qu'à ses objectifs. Cela inclut le point de vue des parties intéressées.

Cela met en œuvre en général une compréhension du terme «risque» qui restreint le concept de risque de l'ISO 31000 en ce sens que l'accent est mis sur l'impact négatif potentiel des écarts par rapport à ce

qui est attendu. Cette approche peut être considérée comme faisant partie de la définition plus large du risque de l'ISO 31000:2018, 3.1.

5 Recommandations relatives à l'ISO 31000 pour les utilisateurs de NSM

L'ISO 31000:2018 propose des recommandations applicables par tous les types d'organismes, quels que soient leur type et leur taille, et s'adresse aux personnes qui, au sein des organismes, créent de la valeur et la préservent par le management du risque, la prise de décision, l'établissement d'une finalité et d'une stratégie, l'atteinte des objectifs et l'amélioration de la performance.

Les huit principes du management du risque servent de fondement à la création et à la préservation de la valeur. Ils fournissent des recommandations sur les caractéristiques d'un management du risque efficace et efficient, en communiquant sa valeur et en expliquant son intention et sa finalité. L'ISO 31000 fournit une approche commune permettant de gérer tout type de risque auquel un organisme est confronté au cours de sa vie.

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 décision.

Il convient d'ajuster le processus de management du risque tel que décrit dans l'ISO 31000 de façon proportionnée au contexte externe et interne de l'organisme et de ses objectifs. Il convient de l'adapter pour qu'il fasse partie intégrante du système de management et qu'il soit intégré dans la structure, le fonctionnement et les processus de l'organisme.

En suivant les recommandations relatives aux principes et au cadre organisationnel, un organisme peut choisir d'ajuster l'application des processus de management du risque à son système de management pour tout type de risque auquel il est confronté au cours de sa vie. Ajouter les étapes du processus de management du risque peut permettre d'améliorer le système de management. Dans ce contexte, il est nécessaire de se rappeler que, bien que le processus de management du risque soit souvent présenté comme séquentiel, dans la pratique, il est itératif.

Il convient d'appliquer le management du risque chaque fois qu'une information ou une estimation quelconque initialise ou alimente un processus ou une activité, ou chaque fois qu'il y a un changement dans le contexte de l'organisme.

Il peut exister un degré d'incertitude dans cette information ou estimation, ce qui peut avoir un effet sur l'atteinte des objectifs. Un effet est expliqué dans l'ISO 31000:2018, 3.1, comme étant un écart par rapport à un attendu, lequel peut être positif, négatif ou les deux à la fois. Par conséquent, il convient que l'organisme revienne sur l'identification du risque chaque fois qu'il dispose de nouvelles informations ou estimations pertinentes pour ses processus et activités.

La Figure 1 montre la correspondance entre les lignes directrices de l'ISO 31000 et le cadre organisationnel des articles génériques de la structure-cadre des NSM. La ligne du haut renvoie aux articles de la structure-cadre tandis que la colonne de gauche représente les articles du cadre organisationnel de l'ISO 31000. Par exemple, si l'on regarde à l'intersection de l'ISO 31000:2018, 5.2, portant sur le leadership et de l'article de la structure-cadre sur le leadership, la zone grise indique la présence d'un processus faisant référence au management du risque. Ce tableau peut donc servir de point de référence. Pour plus de détails sur les relations entre les articles, voir le Tableau A.1.

Figure 1 — Relations entre l'ISO 31000 et les articles de la structure-cadre des NSM

6 Systèmes de management intégrés et utilisation de l'ISO 31000

L'application du management du risque peut se faire par l'approche processus d'un système de management. Il convient de fusionner le cadre organisationnel de l'ISO 31000 avec le système de management en appliquant une analyse des écarts pour inclure les composantes du cadre organisationnel de l'ISO 31000. L'intégration du management du risque dans l'approche processus permet d'éviter les doublons ou les conflits.

Afin de parvenir à une intégration et à une mise en œuvre efficaces et efficientes du cadre organisationnel de l'ISO 31000 et de son processus dans d'autres NSM, il convient que l'organisme adopte les principes de l'ISO 31000. La manuel de l'ISO intitulé *The Integrated Use of Management Systems Standards (IUMSS)* [5] peut être une référence utile à cet égard. Pour connaître les étapes détaillées permettant d'intégrer l'utilisation des NSM, il est conseillé de se reporter à ce manuel.

L'Annexe A fournit des recommandations sur la manière dont un organisme peut aborder l'intégration du management du risque dans ses NSM. L'Annexe B présente une étude de cas sur l'intégration de l'ISO 31000 dans un système de management pluridisciplinaire.

Annexe A
(informative)

Correspondance entre l'ISO 31000 et la structure-cadre des NSM

Le Tableau A.1 montre les liens entre les principaux articles de l'ISO 31000 et les articles corrélés les plus importants de la structure-cadre des NSM. Les utilisateurs de l'ISO 31000 peuvent intégrer les pratiques du management du risque dans le système de management de l'organisme là où les articles de la structure-cadre sont traités.

Tableau A.1 — Correspondance entre l'ISO 31000 et la structure-cadre des NSM

Articles de la structure-cadre des NSM		Articles de l'ISO 31000:2018		
		4. Principes[a]	5. Cadre organisationnel	6. Processus
4. Contexte de l'organisme	4.1 Compréhension de l'organisme et de son contexte	0, a), c), e), f), g)	5.2, 5.4.1	6.1, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.2 Compréhension des besoins et attentes des parties intéressées	0, a), c), d), e), f), g)	5.2, 5.4.1, 5.4.5	6.1, 6.2, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.3 Détermination du périmètre d'application du système de management XXX	0, a), c), f)	5.1, 5.2, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
	4.4 Système de management XXX	0, a), b), c), f)	5.1, 5.2, 5.3, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
5. Leadership	5.1 Leadership et engagement	0, a), c), d), g)	5.1, 5.2, 5.4.2, 5.4.4	6.2, 6.6, 6.7
	5.2 Politique	0, a), c), d), g)	5.2, 5.4.2	6.2, 6.6, 6.7
	5.3 Rôles, responsabilités et autorités au sein de l'organisme	a), c), d), g)	5.2, 5.4.3	—
6. Planification	6.1 Actions à mettre en œuvre face aux risques et opportunités	0, a), b), e), f)	5.1, 5.4.2, 5.7.1	6.1, 6.4, 6.5
	6.2 Objectifs XXX et planification des actions pour les atteindre	0, a), b)	5.4.2, 5.7.2	6.5
7. Soutien	7.1 Ressources	0, a), f), g)	5.1, 5.4.4	6.3.4, 6.5.2
	7.2 Compétences	0, a), f), g)	5.1	—
	7.3 Sensibilisation	0, a), f), g)	5.1	—
	7.4 Communication	0, a), d), f)	5.1, 5.4.5	6.1, 6.2, 6.3.4
	7.5 Informations documentées	0, a), f)	5.1	6.1, 6.7
8. Réalisation des activités opérationnelles	8.1 Planification et maîtrise opérationnelles	0, a), b), f)	5.1, 5.3, 5.5, 5.7	6.1, 6.4, 6.5, 6.6, 6.7

[a] Le principe «0» renvoie au principe de base «création et préservation de la valeur».

NOTE Les numéros de paragraphe dans les cellules renvoient aux paragraphes de l'ISO 31000:2018 en fonction de l'intitulé de la colonne pertinente.