COPYRIGHT NOTICE & TERMS OF USE

SAI GLOBAL, Index House, Ascot, Berks, SL5 7EU, UK
☎: +44 (0)1344 636300. Fax: +44 (0)1344 291194. E-mail: standards@saiglobal.com. www.ili.co.uk

SAI GLOBAL, Forest Road Office Centre, 210 Route 4 East, Paramus, NJ 07652
☎ 201-986-1131. Fax: 201-986-7886. E-mail: sales@ili-info.com. www.ili-info.com

SAI GLOBAL, 286 Sussex Street, Sydney NSW 2000, Australia
☎: +61 2 8206 6060. Fax: +61 2 8206 6019. E-mail: sales@saiglobal.com. www.saiglobal.com

NORME INTERNATIONALE

ISO 31000

Deuxième édition
2018-02

Management du risque — Lignes directrices

Risk management — Guidelines

Numéro de référence
ISO 31000:2018(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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

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.

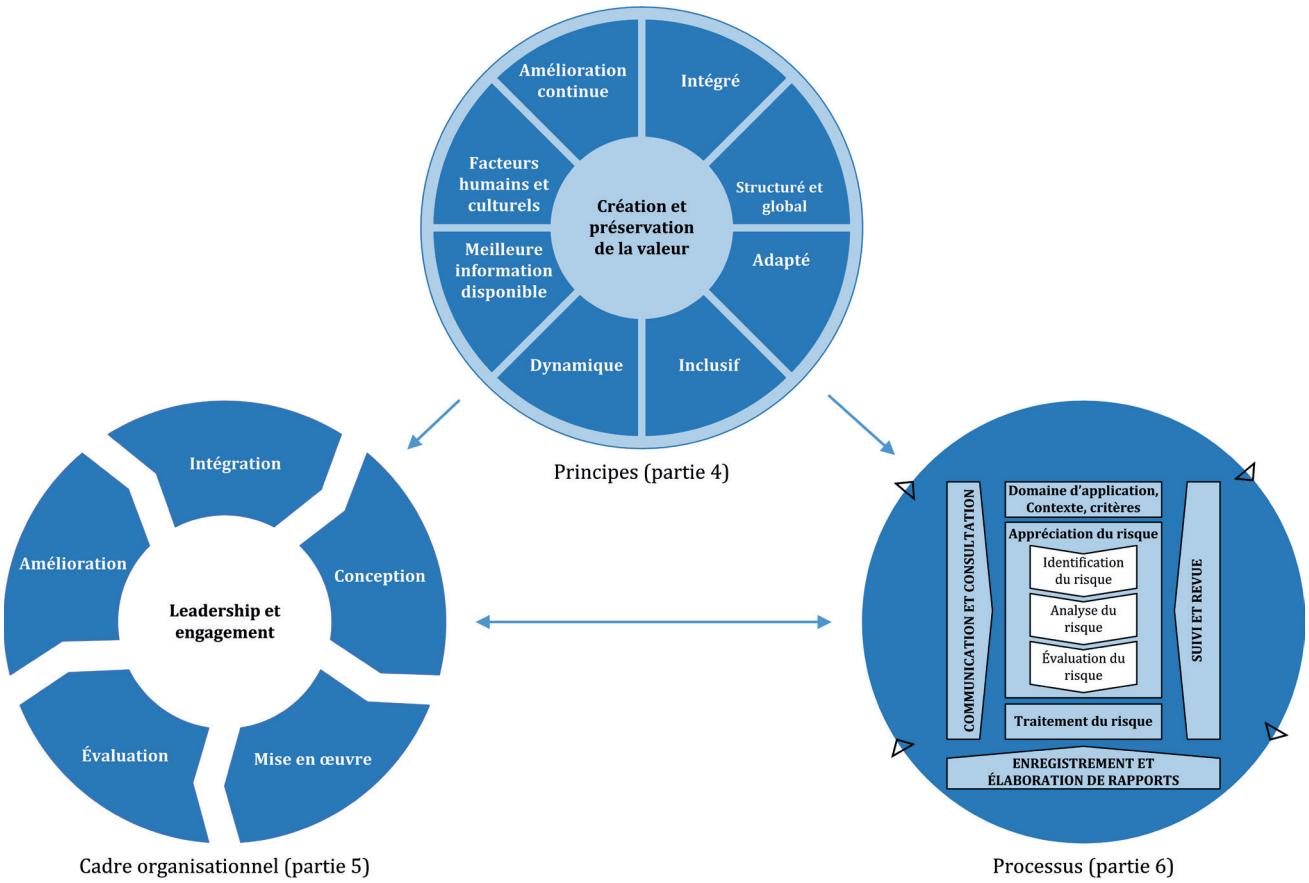

Figure 1 — Principes, cadre organisationnel et processus

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)

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

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).

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.

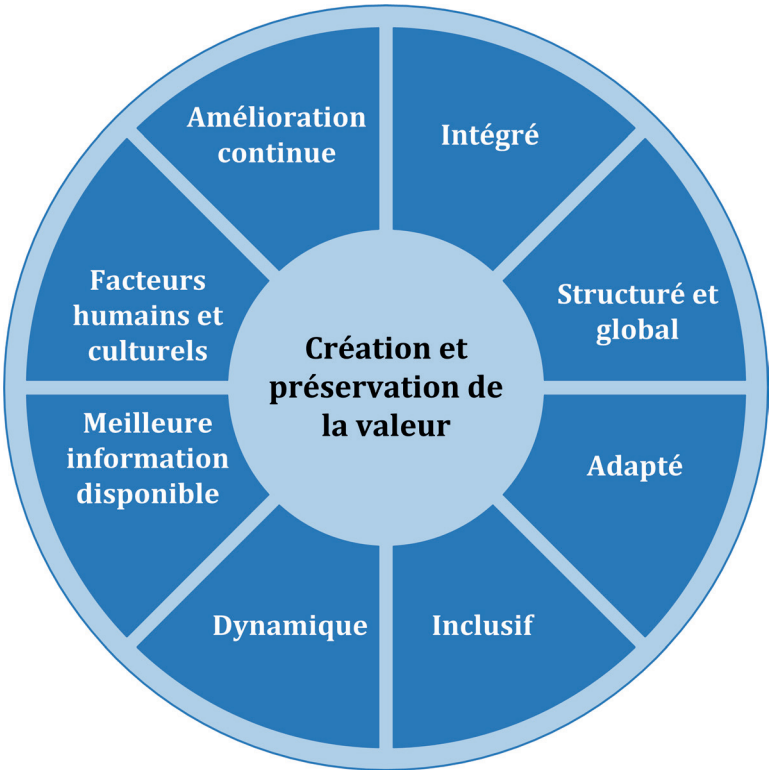

Figure 2 — Principes

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

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

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.

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.

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.

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.

L'intégration du management du risque dans un organisme est un processus dynamique et itératif, qu'il convient d'adapter aux besoins et à la culture de l'organisme. Il convient que le management du risque fasse partie, et ne soit pas séparé, de la finalité, de la gouvernance, du leadership et de l'engagement, de la stratégie, des objectifs et des opérations de l'organisme.

5.4 Conception

5.4.1 Compréhension de l'organisme et de son contexte

Lors de la conception du cadre organisationnel de management du risque, il convient que l'organisme analyse et comprenne son contexte externe et interne.

L'analyse du contexte externe d'un organisme peut comprendre, entre autres:

— les facteurs sociaux, culturels, politiques, légaux, réglementaires, financiers, technologiques, économiques et environnementaux, au niveau international, national, régional ou local;

— les moteurs et tendances clés ayant une incidence sur les objectifs de l'organisme;

— les relations avec les parties prenantes externes, leurs perceptions, leurs valeurs, leurs besoins et leurs attentes;

— les relations contractuelles et les engagements;

— la complexité des réseaux et des dépendances.

L'analyse du contexte interne d'un organisme peut comprendre, entre autres:

— la vision, la mission et les valeurs;

— la gouvernance, l'organisation, les rôles et les responsabilités;

— la stratégie, les objectifs et les politiques;

— la culture de l'organisme;

— les normes, les lignes directrices et les modèles adoptés par l'organisme;

— les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnel, propriété intellectuelle, processus, systèmes et technologies);

— les données, les systèmes d'information et la circulation de l'information;

— les relations avec les parties prenantes internes, en tenant compte de leurs perceptions et de leurs valeurs;

— les relations contractuelles et les engagements;

— les interdépendances et les interconnexions.

5.4.2 Définir clairement l'engagement en matière de management du risque

Il convient que la direction et les organes de surveillance, le cas échéant, démontrent et définissent clairement leur engagement permanent en matière de management du risque par le biais d'une politique, d'une déclaration ou d'autres formes permettant de communiquer clairement les objectifs et l'engagement de l'organisme en matière de management du risque. Il convient que cet engagement comprenne, sans toutefois s'y limiter:

— le but de l'organisme en matière de management du risque et les liens avec ses objectifs et ses autres politiques;

— le rappel de la nécessité d'intégrer le management du risque à la culture globale de l'organisme;

— le pilotage de l'intégration du management du risque dans les principales activités de l'organisme et dans la prise de décisions;

— les pouvoirs et les responsabilités;

— la mise à disposition des ressources nécessaires;

— la manière de traiter des objectifs contradictoires;

— l'évaluation et le compte rendu dans le cadre des indicateurs de performance de l'organisme;

— la revue et l'amélioration.

Il convient que l'engagement en matière de management du risque soit communiqué au sein de l'organisme et aux parties prenantes, le cas échéant.

5.4.3 Attribution des rôles, pouvoirs et responsabilités au sein de l'organisme

Il convient que la direction et les organes de surveillance, le cas échéant, s'assurent que les pouvoirs et responsabilités pour les rôles pertinents en matière de management du risque sont attribués et communiqués à tous les niveaux de l'organisme, et:

— soulignent que le management du risque est une responsabilité fondamentale;

— identifient les personnes ayant la responsabilité du risque et le pouvoir pour le gérer (propriétaires du risque).

5.4.4 Affectation des ressources

Il convient que la direction et les organes de surveillance, le cas échéant, assurent l'affectation des ressources nécessaires au management du risque, ces dernières pouvant comprendre, sans toutefois s'y limiter:

— les personnels, les aptitudes, l'expérience et les compétences;

— les processus, méthodes et outils de l'organisme servant au management du risque;

— les processus et procédures documentés;

— les systèmes de gestion des informations et des connaissances;

— les besoins en perfectionnement et formation professionnels.

Il convient que l'organisme prenne en compte les capacités et les contraintes des ressources existantes.

5.4.5 Établissement d'une communication et d'une concertation

Il convient que l'organisme établisse une méthode de communication et de consultation approuvée afin de soutenir le cadre organisationnel et de faciliter l'application efficace du management du risque. La communication implique de partager des informations avec des publics ciblés. La consultation implique également un retour d'information des participants dans l'espoir qu'il contribue aux décisions ou à d'autres activités et les oriente. Il convient que les méthodes et le contenu de la communication et de la consultation reflètent les attentes des parties prenantes, le cas échéant.

Il convient que la communication et la consultation aient lieu en temps utile et permettent que les informations pertinentes soient collectées, consolidées, synthetisées et partagées de manière appropriée, qu'un retour d'information soit fait et que des améliorations soient apportées.

5.5 Mise en œuvre

Il convient que l'organisme mette en œuvre le cadre organisationnel de management du risque en:

— élaborant un plan approprié comprenant un calendrier et des ressources;

— identifiant où, quand et comment les différents types de décisions sont prises au sein de l'organisme, et par qui;

— modifiant les processus décisionnels applicables si nécessaire;

— s'assurant que les dispositions de l'organisme en matière de management du risque sont clairement comprises et mises en œuvre.

Le succès de la mise en œuvre du cadre organisationnel requiert l'implication et la sensibilisation des parties prenantes. Cela permet aux organismes de traiter explicitement de l'incertitude dans la prise de décisions, tout en s'assurant que toute incertitude nouvelle ou ultérieure puisse être prise en compte lorsqu'elle apparaît.

Conçu et mis en œuvre de façon appropriée, le cadre organisationnel de management du risque garantira que le processus de management du risque fait partie intégrante de toutes les activités à tous les niveaux de l'organisme, y compris la prise de décisions, et que les changements intervenant dans les contextes externe et interne seront suivis de manière adéquate.

5.6 Évaluation

Pour évaluer l'efficacité du cadre organisationnel de management du risque, il convient que l'organisme:

— mesure périodiquement les performances du cadre organisationnel de management du risque par rapport à sa finalité, aux plans de mise en œuvre, aux indicateurs et au comportement attendu;

— détermine s'il demeure pertinent pour aider à atteindre les objectifs de l'organisme.

5.7 Amélioration

5.7.1 Adaptation

Il convient que l'organisme surveille en continu et adapte le cadre organisationnel de management du risque en fonction des changements externes et internes. L'organisme peut ainsi améliorer sa valeur.

5.7.2 Amélioration continue

Il convient que l'organisme améliore en continu la pertinence, l'adéquation et l'efficacité du cadre organisationnel de management du risque et la façon dont le processus de management du risque est intégré.

Lorsque des lacunes ou des opportunités d'amélioration sont identifiées, il convient que l'organisme élabore des plans et définisse des tâches, et les attribue aux responsables de leur mise en œuvre. Une fois mises en œuvre, il convient que ces améliorations contribuent au renforcement du management du risque.

6 Processus

6.1 Généralités

Le processus de management du risque implique l'application systématique de politiques, de procédures et de pratiques aux activités de communication et de consultation, d'établissement du contexte et d'appréciation, de traitement, de suivi, de revue, d'enregistrement et de compte rendu du risque. Ce processus est illustré à la Figure 4.

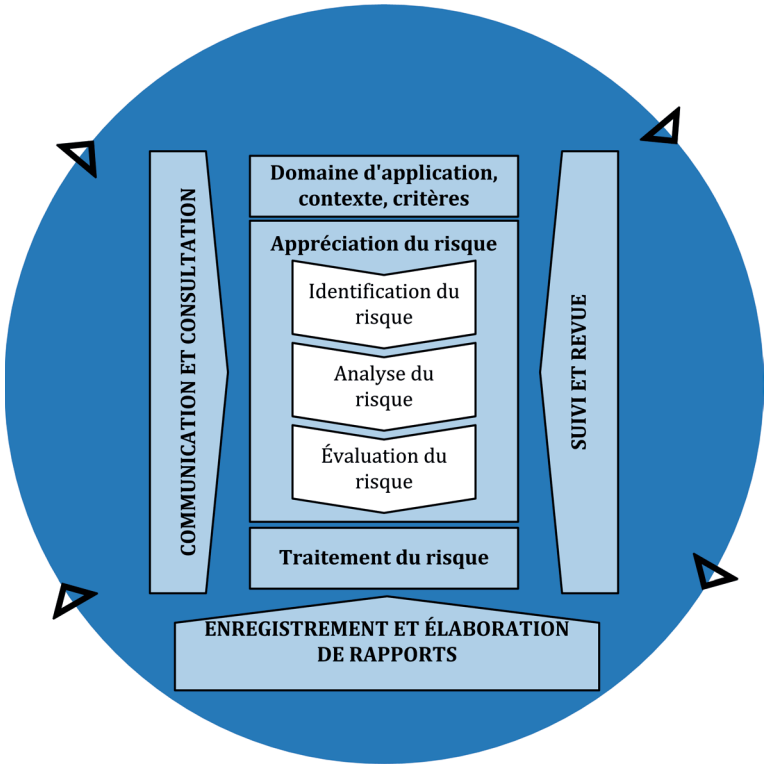

Figure 4 — Processus

Il convient que le processus de management du risque fasse partie intégrante du management et de la prise de décisions et soit intégré à la structure, aux opérations et aux processus de l'organisme. Il peut être appliqué aux niveaux stratégique, opérationnel, programme ou projet.

Il peut y avoir de nombreuses applications du processus de management du risque au sein d'un organisme, adaptées pour atteindre des objectifs en fonction du contexte externe et interne dans lequel elles s'appliquent.

Il convient de prendre en compte la nature dynamique et variable du comportement humain et de la culture tout au long du processus de management du risque.

Bien que le processus de management du risque soit souvent présenté comme un processus séquentiel, dans la pratique, il est itératif.

6.2 Communication et consultation

La communication et la consultation ont pour but d'aider les parties prenantes pertinentes à comprendre le risque, les principes de prise de décisions et les raisons pour lesquelles certaines actions sont nécessaires. La communication vise à accroître la sensibilisation et la compréhension du risque, alors que la consultation implique l'obtention d'un retour et d'informations pour étayer la prise de décisions. Une étroite coordination entre les deux facilite des échanges d'informations factuels, opportuns, pertinents, précis et compréhensibles tout en prenant en compte la confidentialité et l'intégrité des informations ainsi que le droit à la vie privée des personnes.

Il convient que la communication et la consultation avec les parties prenantes internes et externes concernées aient lieu à toutes les étapes du processus de management du risque.

La communication et la consultation visent à:

— réunir différents domaines d'expertise pour chaque étape du processus de management du risque;

— s'assurer que les différents points de vue sont pris en compte de manière appropriée dans la définition des critères de risque et lors de l'évaluation des risques;

— fournir suffisamment d'informations pour faciliter la surveillance du risque et la prise de décisions;

— faire naître un sentiment d'inclusion et de propriété parmi ceux affectés par le risque.

6.3 Périmètre d'application, contexte et critères

6.3.1 Généralités

L'établissement du périmètre d'application, du contexte et des critères a pour but d'adapter le processus de management du risque, en permettant une appréciation du risque efficace et un traitement du risque approprié. Le périmètre d'application, le contexte et les critères impliquent de définir le périmètre d'application du processus et de comprendre le contexte interne et externe.

6.3.2 Définition du domaine d'application

Il convient que l'organisme définisse le périmètre d'application de ses activités de management du risque.

Le processus de management du risque pouvant être appliqué à différents niveaux (par exemple au niveau de la stratégie, des opérations, d'un programme, d'un projet ou d'autres activités), il est important d'être précis quant au domaine d'application considéré, aux objectifs pertinents à prendre en compte et à leur alignement sur les objectifs de l'organisme.

Lors de la planification de l'approche, les éléments à prendre en compte comprennent:

— les objectifs et les décisions à prendre;

— les résultats attendus des étapes du processus;

— le temps, l'emplacement, les inclusions et exclusions spécifiques;

— les outils et techniques appropriés d'appréciation du risque;

— les ressources nécessaires, les responsabilités et la documentation à établir;

— les relations avec d'autres projets, processus et activités.

6.3.3 Contexte interne et externe

Le contexte interne et externe est l'environnement dans lequel l'organisme cherche à définir et atteindre ses objectifs.

Il convient que le contexte du processus de management du risque soit établi à partir de la compréhension de l'environnement externe et interne dans lequel opère l'organisme et qu'il reflète l'environnement spécifique de l'activité à laquelle le processus de management du risque doit être appliqué.

La compréhension du contexte est importante car:

— le management du risque a lieu dans le contexte des objectifs et des activités de l'organisme;

— les facteurs organisationnels peuvent être une source de risque;

— la finalité et le domaine d'application du processus de management du risque peuvent être corrélés aux objectifs de l'organisme dans son ensemble.

Il convient que l'organisme établisse le contexte externe et interne du processus de management du risque en tenant compte des facteurs mentionnés en 5.4.1.

6.3.4 Définition des critères de risque

Il convient que l'organisme spécifie le niveau et le type de risque pouvant ou non être pris par l'organisme, en fonction des objectifs. Il convient également qu'il définisse des critères permettant d'évaluer l'importance du risque et d'étayer les processus décisionnels. Il convient que les critères de risque soient alignés sur le cadre organisationnel de management du risque et adaptés à la finalité et au domaine d'application spécifique de l'activité considérée. Il convient que les critères de risque reflètent les valeurs, les objectifs et les ressources de l'organisme et soient cohérents avec les politiques et déclarations en matière de management du risque. Il convient que les critères soient définis en tenant compte des obligations de l'organisme et de l'opinion des parties prenantes.

Bien qu'il convienne d'établir les critères de risque au début du processus d'appréciation du risque, ces critères sont dynamiques et il convient qu'ils soient revus en permanence et modifiés si nécessaire.

Pour fixer les critères de risque, il convient de prendre en compte les éléments suivants:

— la nature et le type d'incertitudes pouvant avoir une incidence sur les résultats et les objectifs (tangibles et intangibles);

— la façon dont les conséquences (positives et négatives) et la vraisemblance seront définies et mesurées;

— les facteurs liés au temps;

— la cohérence dans l'utilisation des mesures;

— la méthode de détermination du niveau de risque;

— la façon dont les combinaisons et séquences de plusieurs risques seront prises en compte;

— la capacité de l'organisme.

6.4 Appréciation du risque

6.4.1 Généralités

L'appréciation du risque est le processus global d'identification, d'analyse et d'évaluation du risque.

Il convient que l'appréciation du risque soit menée de façon systématique, itérative et collaborative, en s'appuyant sur les connaissances et les opinions des parties prenantes. Il convient d'utiliser les meilleures informations disponibles, complétées si nécessaire par une enquête plus approfondie.

6.4.2 Identification du risque

L'identification du risque a pour but de rechercher, reconnaître et décrire les risques qui peuvent aider ou empêcher un organisme d'atteindre ses objectifs. Il est essentiel que les informations utilisées pour l'identification des risques soient pertinentes, appropriées et à jour.

L'organisme peut utiliser un éventail de techniques pour identifier les incertitudes pouvant avoir une incidence sur un ou plusieurs objectifs. Il convient de prendre en compte les facteurs suivants et leurs relations:

— sources de risque tangibles et intangibles;

— causes et événements;

— menaces et opportunités;

— vulnérabilités et capacités;

— changements intervenus au niveau du contexte externe et interne;

— indicateurs de risques émergents;

— nature et valeur des actifs et des ressources;

— conséquences et leur impact sur les objectifs;

— limitations des connaissances et fiabilité des informations;

— facteurs liés au temps;

— biais, hypothèses et convictions des personnes impliquées.

Il convient que l'organisme identifie les risques, que leurs sources soient ou non sous son contrôle. Il convient de tenir compte du fait qu'il peut y avoir plusieurs types de résultat pouvant avoir diverses conséquences tangibles ou intangibles.

6.4.3 Analyse du risque

L'analyse du risque a pour but de comprendre la nature du risque et ses caractéristiques, y compris le niveau de risque, le cas échéant. L'analyse du risque implique la prise en compte détaillée des incertitudes, des sources de risque, des conséquences, de la vraisemblance, des événements, des scénarios, des moyens de maîtrise et de leur efficacité. Un événement peut avoir des causes et conséquences multiples et affecter des objectifs multiples.

L'analyse du risque peut être menée à différents niveaux de détail et de complexité selon la finalité de l'analyse, la disponibilité et la fiabilité des informations et les ressources disponibles. Les techniques d'analyse peuvent être qualitatives, quantitatives, ou une combinaison de celles-ci, selon les circonstances et l'utilisation prévue.

Il convient que l'analyse du risque prenne en compte des facteurs tels que:

— la vraisemblance des événements et des conséquences;

— la nature et l'importance des conséquences;

— la complexité et l'interconnexion;

— les facteurs liés au temps et la volatilité;

— l'efficacité des moyens de maîtrise existants;

— les niveaux de sensibilité et de confiance.

L'analyse du risque peut être influencée par toute divergence d'opinions, biais, perceptions du risque et jugements. Les influences supplémentaires sont la qualité des informations utilisées, les hypothèses et exclusions posées, toute limitation des techniques et la façon dont elles sont mises en œuvre. Il convient que ces influences soient prises en compte, documentées et communiquées aux décideurs.

Les événements extrêmement incertains peuvent être difficiles à quantifier. Cela peut poser problème lors de l'analyse d'événements ayant de graves conséquences. Dans de tels cas, l'utilisation d'une combinaison de techniques permet généralement d'acquérir une connaissance plus approfondie.

L'analyse du risque fournit des données permettant d'évaluer le risque, de prendre la décision de le traiter ou non et de quelle manière, et permet de choisir la stratégie et les méthodes de traitement les plus performantes. Les résultats fournissent des renseignements en vue des décisions quand il faut effectuer des choix et que les options impliquent différents types et niveaux de risque.

6.4.4 Évaluation du risque

L'évaluation du risque a pour but de déboucher sur des décisions plus judicieuses. L'évaluation du risque consiste à comparer les résultats de l'analyse du risque aux critères de risque établis afin de déterminer si une action supplémentaire est exigée. Cela peut déboucher sur la décision:

— de ne rien faire de plus;

— d'examiner les options de traitement du risque;

— d'entreprendre une analyse plus approfondie afin de mieux comprendre le risque;

— de maintenir les moyens de maîtrise du risque existants;

— de réexaminer les objectifs.

Il convient que les décisions prennent en compte un contexte plus large et les conséquences réelles et perçues pour les parties prenantes externes et internes.

Il convient que le résultat de l'évaluation du risque soit enregistré, communiqué, puis validé aux niveaux appropriés de l'organisme.

6.5 Traitement du risque

6.5.1 Généralités

Le traitement du risque a pour but de choisir et de mettre en œuvre des options pour aborder le risque.

Le traitement du risque implique un processus itératif:

— formuler et choisir des options de traitement du risque;

— élaborer et mettre en œuvre le traitement du risque;

— apprécier l'efficacité de ce traitement;

— déterminer si le risque résiduel est acceptable;

— s'il n'est pas acceptable, envisager un traitement complémentaire.

6.5.2 Sélection des options de traitement du risque

Le choix de la ou des options de traitement du risque les plus appropriées implique de comparer les avantages potentiels en termes d'atteinte des objectifs par rapport aux coûts, aux efforts et aux inconvénients de leur mise en œuvre.

Les options de traitement du risque ne s'excluent pas nécessairement les unes les autres, et ne sont pas appropriées à toutes les situations. Les options de traitement du risque peuvent impliquer un ou plusieurs des éléments suivants:

— un refus du risque marqué par la décision de ne pas commencer ou poursuivre l'activité porteuse du risque;

— la prise ou l'augmentation d'un risque afin de saisir une opportunité;

— l'élimination de la source de risque;

— une modification de la vraisemblance;

— une modification des conséquences;

— un partage du risque (par exemple par le biais de contrats, de souscription de couvertures d'assurance);

— un maintien du risque fondé sur une décision éclairée.

La justification d'un traitement du risque dépasse le cadre des seules considérations économiques et il convient de prendre en compte toutes les obligations de l'organisme, ses engagements d'autres natures et l'opinion des parties prenantes. Il convient de choisir les options de traitement du risque en fonction des objectifs de l'organisme, des critères de risque et des ressources disponibles.

Lors du choix des options de traitement du risque, il convient que l'organisme tienne compte des valeurs, des perceptions et de l'implication potentielle des parties prenantes et examine les moyens les plus appropriés de communiquer et de les consulter. À efficacité égale, certains traitements du risque peuvent être plus acceptables que d'autres pour certaines parties prenantes.

Les traitements du risque, même s'ils sont soigneusement conçus et mis en œuvre, peuvent ne pas produire les résultats escomptés et avoir des conséquences inattendues. Pour s'assurer que les différentes formes de traitement sont et restent efficaces, le suivi et la revue doivent faire partie intégrante de la mise en œuvre du traitement du risque.

Le traitement du risque peut également engendrer de nouveaux risques qui doivent être gérés.

S'il n'existe aucune option de traitement disponible ou si les options de traitement ne permettent pas de modifier suffisamment le risque, il convient que le risque soit enregistré et mis sous contrôle de façon permanente.

Il convient que les décideurs et les autres parties prenantes soient informés de la nature et de l'étendue du risque résiduel après le traitement du risque. Il convient que le risque résiduel soit documenté et soumis à suivi et revue et, le cas échéant, fasse l'objet d'un traitement supplémentaire.

6.5.3 Élaboration et mise en œuvre des plans de traitement du risque

Les plans de traitement du risque ont pour but de préciser la manière dont les options de traitement choisies seront mises en œuvre de sorte que les dispositions soient comprises par les personnes concernées et que les progrès par rapport au plan puissent faire l'objet d'un suivi. Il convient que le plan de traitement identifie clairement l'ordre de mise en œuvre du traitement du risque.

Il convient que les plans de traitement soient intégrés aux plans et processus de management de l'organisme, en concertation avec les parties prenantes appropriées.

Il convient que les informations fournies dans le plan de traitement comportent:

— la justification du choix des options de traitement, y compris les avantages attendus;

— les personnes responsables de l'approbation et de la mise en œuvre du plan;

— les actions proposées;

— les ressources nécessaires, en tenant compte des imprévus;

— les mesures des performances;

— les contraintes;

— les rapports et le suivi requis;

— le moment où les actions sont censées être entreprises et achevées.

6.6 Suivi et revue

Le suivi et la revue ont pour but de s'assurer et d'améliorer la qualité et l'efficacité de la conception, de la mise en œuvre et des résultats du processus. Il convient que le suivi continu et la revue périodique

du processus de management du risque et de ses résultats soient planifiés dans le processus de management du risque, en définissant clairement les responsabilités.

Il convient que le suivi et la revue aient lieu à toutes les étapes du processus. Le suivi et la revue comprennent la planification, le recueil et l'analyse d'informations, l'enregistrement des résultats et le retour d'information.

Il convient d'intégrer les résultats du suivi et de la revue aux activités de management des performances de l'organisme, de suivi des résultats et d'élaboration de rapports.

6.7 Enregistrement et élaboration de rapports

Il convient que le processus de management du risque et ses résultats soient documentés et fassent l'objet de rapports selon des mécanismes appropriés. L'enregistrement et l'élaboration de rapports a pour but de:

— communiquer sur les activités de management du risque et leurs résultats au sein de l'organisme;

— fournir des informations en vue de la prise de décisions;

— améliorer les activités de management du risque;

— faciliter l'interaction avec les parties prenantes, y compris celles ayant la responsabilité des activités de management du risque.

Il convient que les décisions concernant la création, la conservation et le traitement des informations documentées tiennent compte, sans toutefois s'y limiter, de leur utilisation, du caractère sensible des informations et du contexte externe et interne.

L'élaboration de rapports fait partie intégrante de la gouvernance de l'organisme et il convient qu'elle améliore la qualité du dialogue avec les parties prenantes et aide la direction et les organes de surveillance à faire face à leurs responsabilités. Les facteurs à prendre en considération pour l'établissement de rapports comprennent, sans toutefois s'y limiter:

— les différentes parties prenantes et leurs besoins et exigences spécifiques en matière d'information;

— le coût, la fréquence et le caractère opportun de l'établissement de rapports;

— la méthode adoptée pour l'établissement de rapports;

— la pertinence des informations au regard des objectifs de l'organisme et de la prise de décisions.

Bibliographie

[1] IEC 31010, *Gestion des risques — Techniques d'évaluation des risques*

ICS 03.100.01

Prix basé sur 16 pages