NF ISO 31000

2010-01

Contacter :
AFNOR – Norm'Info
11, rue Francis de Pressensé
93571 La Plaine Saint-Denis Cedex
Tél : 01 41 62 76 44
Fax : 01 49 17 92 02
E-mail : norminfo@afnor.org

FA153460 ISSN 0335-3931

norme française

NF ISO 31000

Janvier 2010

Indice de classement : **X 50-254**

ICS : 03.100.01

Management du risque

Principes et lignes directrices

E : Risk management — Principles and guidelines
D : Risikomanagement — Allgemeine Anleitung zu den Grundsätzen und zur Implementierung eines Risikomanagements

Norme française homologuée

par décision du Directeur Général d'AFNOR le 30 décembre 2009 pour prendre effet le 30 janvier 2010.

Correspondance

Le présent document reproduit intégralement la Norme internationale ISO 31000:2009.

Analyse

Le présent document fournit des principes et des lignes directrices générales sur le management du risque.

Ce document peut être appliqué par tout public, toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu. Par conséquent, il n'est pas spécifique à une industrie ou un secteur donné.

Il peut être appliqué tout au long de la vie d'un organisme et à une large gamme d'activités, dont les stratégies et les prises de décisions, les activités opérationnelles, les processus, les fonctions, les projets, les produits, les services et les actifs.

Le présent document n'a pas vocation à servir de base à une certification.

Descripteurs

Thésaurus International Technique : entreprise, planification, gestion, risque, norme, utilisation, réglementation, prévention des accidents, sécurité, organisation, efficacité, processus, code de bonnes pratiques, service, information, mise en œuvre.

Modifications

Corrections

Éditée et diffusée par l'Association Française de Normalisation (AFNOR) — 11, rue Francis de Pressensé — 93571 La Plaine Saint-Denis Cedex
Tél. : + 33 (0)1 41 62 80 00 — Fax : + 33 (0)1 49 17 90 00 — www.afnor.org

Management des risques AFNOR CN RISQUE

Membres de la commission de normalisation

Président : M PEYROUTY

Secrétariat : M BOUCHER — AFNOR

MME	BERGER	AFNOR CERTIFICATION
M	BOYER-VIDAL	GDF SUEZ
M	CERF	ENVA — ECOLE NAT VETERINAIRE ALFORT
M	CHETRIT	TOTAL SA
M	CLAIR	CNPP ENTREPRISE
M	DALI	ATLASCOPE
M	DE MIRAMON	IMDR — INSTITUT POUR LA MAITRISE DES RISQUES
M	DE WISPELAERE	CSP — COMMUNICATION STRUCTURE PERFECT
M	DEBRAY	INERIS
M	DEFRANCE	AFNOR COMPETENCES
M	DELEUZE	EDF R&D
M	DENNERY	GDF SUEZ
M	DESJARDIN	CSP
M	DUBOST	GDF SUEZ — MISSION NORMALISATION
M	DUPAS	STORENGY
M	FAURE	SERNOPTES
M	FILHOL	SNCF
M	GAILLARD	CNES
MME	GAUVAIN	AFNOR CERTIFICATION
MME	GINESTY	DIRECTION GÉNÉRALE DU TRAVAIL
M	GOARANT	AGMS
M	GRALL	SGDN
M	GUILLAUME	SINEQUA RISK & MANAGEMENT
M	HONNAERT	AFNOR COMPETENCES
M	JALINAUD	CEA DAM ILE DE FRANCE
M	JANIAUT	AREVA RISK MANAGEMENT CONSULTING SAS
M	LACQUEMANT	CEA CADARACHE
M	LAHAYE	INERIS
M	LE PAGE	CRAM ILE DE FRANCE
M	LEMARCIS	SNCF
M	LEROUX	ECOLE CENTRALE PARIS
M	LICATA-MESSANA	LRQA FRANCE SAS
M	LOUISOT	JEAN-PAUL LOUISOT
M	LUIZARD	SINEQUA RISK & MANAGEMENT
MME	MARCOU-CHERDEL	EFS — ETS FRANCAIS DU SANG
MME	MIGNARD	CSP
M	MOLINES	MOLINES CONSULTANTS
M	MOTET	INSA
M	O'BRIEN	GROUPE ESAIP
M	OLLIVIER	MUTUELLE BLEUE
M	PAUMARD	TOTAL
M	PELLETIER	COLT TELECOMMUNICATIONS FRANCE
M	PEYROUTY	IRSN
M	POZZANA	TOTAL SA
MME	PRETTO	DIRECTION GÉNÉRALE DU TRAVAIL
M	REMOUE	MEDEF
M	REPUSSARD	IRSN
M	ROBERT	AFNOR DEVELOPPEMENT
MME	ROI	SAFRAN SA
MME	VO DUY	UTC — UNIVERSITE TECHNOLOGIE COMPIEGNE

Sommaire

Page

Avant-propos ..... **iv**

Introduction ..... **v**

1 Domaine d'application **1**

2 Termes et définitions **1**

3 Principes **7**

4 Cadre organisationnel **8**
4.1 Généralités **8**
4.2 Mandat et engagement **9**
4.3 Conception du cadre organisationnel de management du risque **10**
4.3.1 Compréhension de l'organisme et de son contexte **10**
4.3.2 Établissement de la politique de management du risque **10**
4.3.3 Responsabilité **11**
4.3.4 Intégration aux processus organisationnels **11**
4.3.5 Ressources **11**
4.3.6 Établissement de mécanismes de communication et de rapports internes **12**
4.3.7 Établissement de mécanismes de communication et de rapports externes **12**
4.4 Mise en œuvre du management du risque **12**
4.4.1 Mise en œuvre du cadre organisationnel de management du risque **12**
4.4.2 Mise en œuvre du processus de management du risque **13**
4.5 Surveillance et revue du cadre organisationnel **13**
4.6 Amélioration continue du cadre organisationnel **13**

5 Processus **13**
5.1 Généralités **13**
5.2 Communication et concertation **14**
5.3 Établissement du contexte **15**
5.3.1 Généralités **15**
5.3.2 Établissement du contexte externe **15**
5.3.3 Établissement du contexte interne **15**
5.3.4 Établissement du contexte du processus de management du risque **16**
5.3.5 Définition des critères de risque **17**
5.4 Appréciation du risque **17**
5.4.1 Généralités **17**
5.4.2 Identification du risque **17**
5.4.3 Analyse du risque **18**
5.4.4 Évaluation du risque **18**
5.5 Traitement du risque **19**
5.5.1 Généralités **19**
5.5.2 Sélection des options de traitement du risque **19**
5.5.3 Élaboration et mise en œuvre des plans de traitement du risque **20**
5.6 Surveillance et revue **20**
5.7 Enregistrement du processus de management du risque **21**

Annexe A (informative) **Attributs d'un management du risque élevé** **22**

Bibliographie **24**

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 Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

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.

L'ISO 31000 a été élaborée par le groupe de travail du Bureau de gestion technique ISO sur le Management du risque.

Introduction

Les organismes de tous types et de toutes dimensions confrontés à des facteurs et des influences internes et externes ignorent si et quand ils vont atteindre leurs objectifs. L'incidence de cette incertitude sur l'atteinte des objectifs d'un organisme constitue le «risque».

Toutes les activités d'un organisme comprennent des risques. Les organismes gèrent le risque en l'identifiant, en l'analysant, et en évaluant ensuite la nécessité de le modifier par un traitement afin de satisfaire aux critères de risque. Tout au long de ce processus, ils communiquent et se concertent avec les parties prenantes, et surveillent et revoient le risque et les moyens de maîtrise qui modifient le risque afin de s'assurer qu'il n'est pas nécessaire de recourir à un traitement supplémentaire du risque. La présente Norme internationale décrit ce processus systématique et logique en détail.

Alors que tous les organismes gèrent des risques à différents niveaux, la présente Norme internationale fixe un certain nombre de principes qui doivent être appliqués pour rendre le management du risque efficace. La présente Norme internationale recommande que les organismes élaborent, mettent en œuvre et améliorent continuellement un cadre organisationnel dont le but est d'intégrer le processus de management du risque aux processus de gouvernance, de stratégie et de planification, de management, de rédaction des rapports, ainsi qu'aux politiques, aux valeurs et à la culture d'ensemble de l'organisme.

Le management du risque peut s'appliquer à l'ensemble de l'organisme, dans tous ses domaines et à tous ses niveaux, à tout moment, ainsi qu'à des fonctions, des projets et des activités particulières.

Même si la pratique du management du risque s'est développée au fil du temps et dans de nombreux secteurs pour répondre à différents besoins, l'adoption de processus cohérents dans un cadre organisationnel complet peut contribuer à garantir que le risque est géré de façon efficace, performante et cohérente au sein d'un organisme. L'approche générique décrite dans la présente Norme internationale fournit des principes et des lignes directrices pour gérer toute forme de risque de manière systématique, transparente et fiable, dans quelque domaine et quelque contexte que ce soit.

Chaque secteur ou application particulier du management du risque comporte des besoins, des publics, des perceptions et des critères qui lui sont propres. C'est pourquoi, l'un des points essentiels de la présente Norme internationale est d'intégrer «l'établissement du contexte» en tant qu'activité de départ du processus générique de management du risque. Établir le contexte va permettre d'appréhender les objectifs de l'organisme, l'environnement dans lequel il poursuit ces objectifs, les parties prenantes et la diversité des critères de risques, tous ces éléments devant contribuer à révéler et apprécier la nature et la complexité de ses risques.

La Figure 1 illustre les relations entre les principes de management du risque, le cadre organisationnel dans lequel il se présente et le processus de management du risque décrits dans la présente Norme internationale.

La mise en œuvre et le maintien du management du risque conformément à la présente Norme internationale permettent, par exemple, à un organisme

— d'accroître la vraisemblance d'atteindre les objectifs,

— d'encourager un management proactif,

— de prendre conscience de la nécessité d'identifier et de traiter le risque à travers tout l'organisme,

— d'améliorer l'identification des opportunités et des menaces,

— de se conformer aux obligations légales et réglementaires ainsi qu'aux normes internationales,

— d'améliorer la rédaction des rapports obligatoires et volontaires,

— d'améliorer la gouvernance,

— d'accroître l'assurance et la confiance des parties prenantes,

— d'établir une base fiable pour la prise de décision et la planification,

— d'améliorer les moyens de maîtrise,

— d'allouer et d'utiliser efficacement les ressources pour le traitement du risque,

— d'améliorer l'efficacité et l'efficience opérationnelles,

— de renforcer les performances en matière de santé et de sécurité, ainsi que de protection environnementale,

— d'améliorer la prévention des pertes et le management des incidents,

— de minimiser les pertes,

— d'améliorer l'apprentissage organisationnel, et

— d'améliorer la résilience organisationnelle.

La présente Norme internationale est destinée à répondre aux besoins d'une grande diversité de parties prenantes, dont

a) les personnes responsables de l'élaboration d'une politique de management du risque au sein de leur organisme,

b) les personnes chargées de s'assurer que ce risque est géré efficacement au sein de l'organisme dans son ensemble ou dans un domaine, une activité ou un projet spécifique,

c) les personnes chargées d'évaluer l'efficacité d'un organisme en matière de management du risque, et

d) les rédacteurs de normes, guides, procédures et bonnes pratiques qui, en totalité ou en partie, déterminent la manière dont le risque doit être géré dans le contexte spécifique de ces documents.

Les pratiques et processus de management en cours dans nombre d'organismes comportent des éléments de management du risque, et beaucoup d'organismes ont déjà adopté un processus formalisé de management du risque pour des types particuliers de risques ou de situations. Dans de tels cas, un organisme peut décider de réaliser une revue critique de ses pratiques et processus existants à la lumière de la présente Norme internationale.

Dans la présente Norme internationale les expressions «management du risque» et «gérer le risque» sont toutes deux utilisées. De façon générale, le «management du risque» se réfère à la structure (principe, cadre organisationnel et processus) permettant de gérer le risque avec efficacité, alors que «gérer le risque» se réfère à l'application de cette structure aux risques particuliers.

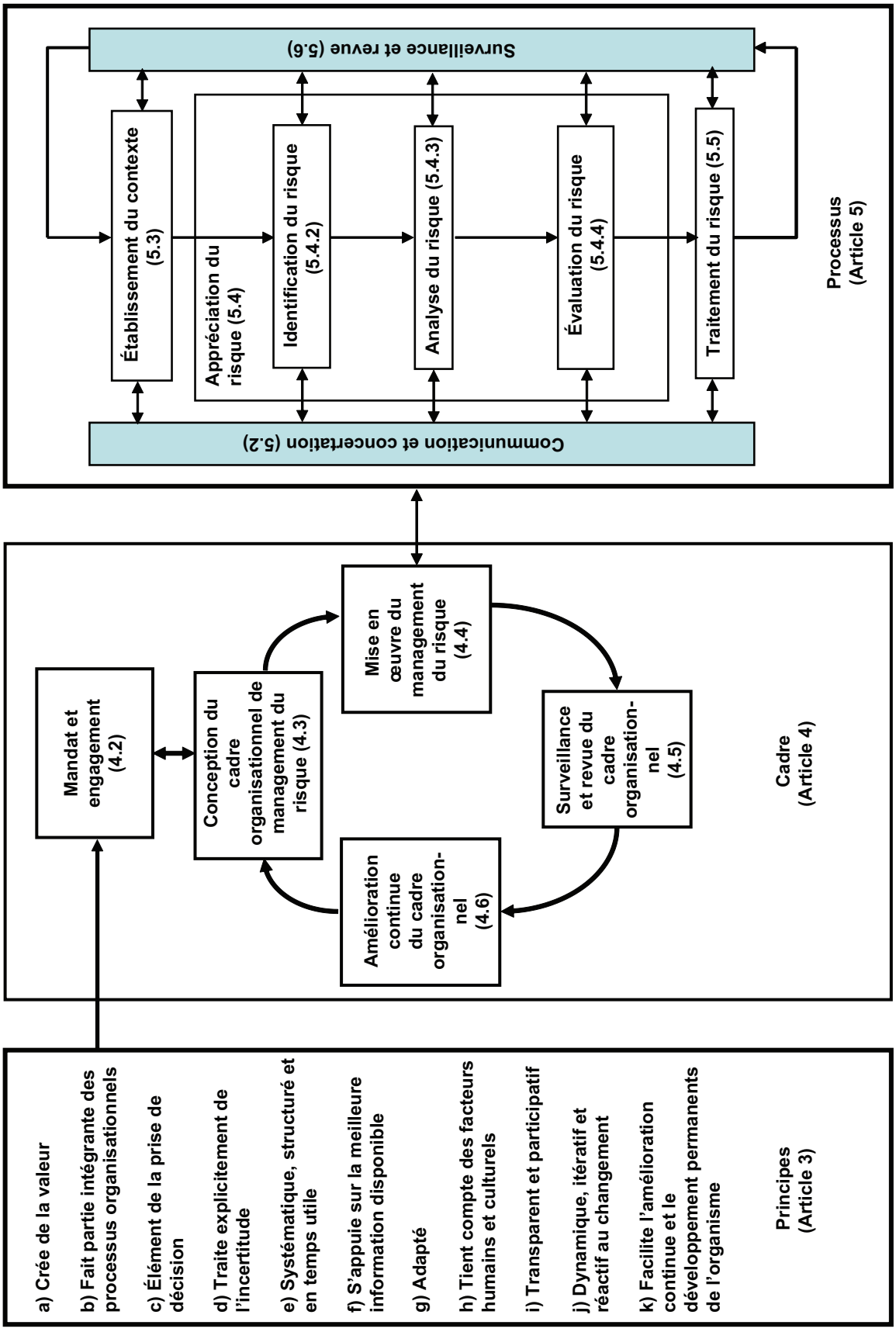

Figure 1 — Relations entre les principes, le cadre organisationnel et le processus de management du risque

Management du risque — Principes et lignes directrices

1 Domaine d'application

La présente Norme internationale fournit des principes et des lignes directrices générales sur le management du risque.

La présente Norme internationale peut être appliquée par tout public, toute entreprise publique ou privée, toute collectivité, toute association, tout groupe ou individu. Par conséquent, la présente Norme internationale n'est pas spécifique à une industrie ou un secteur donné.

NOTE Pour plus de facilité, les différents utilisateurs de la présente Norme internationale sont désignés par le terme général d'«organisme».

La présente Norme internationale peut être appliquée tout au long de la vie d'un organisme et à une large gamme d'activités, dont les stratégies et les prises de décisions, les activités opérationnelles, les processus, les fonctions, les projets, les produits, les services et les actifs.

La présente Norme internationale peut s'appliquer à tout type de risque, quelle que soit sa nature, que ses conséquences soient positives ou négatives.

Bien que la présente Norme internationale fournisse des lignes directrices générales, elle ne vise pas à promouvoir l'uniformisation du management du risque au sein des organismes. La conception et la mise en œuvre des plans et des structures organisationnelles de management du risque devront tenir compte des divers besoins d'un organisme spécifique, de ses objectifs, son contexte, sa structure, son activité, ses processus, ses fonctions, ses projets, ses produits, ses services ou ses actifs particuliers, ainsi que de ses pratiques spécifiques.

Il est prévu que la présente Norme internationale serve à harmoniser les processus de management du risque dans les normes existantes et à venir. Elle offre une approche commune à l'établissement des normes traitant de risques et/ou secteurs spécifiques, sans toutefois remplacer ces normes.

La présente Norme internationale n'a pas vocation à servir de base à une certification.

2 Termes et définitions

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

2.1
risque
effet de l'incertitude sur l'atteinte des objectifs

NOTE 1 Un effet est un écart, positif et/ou négatif, par rapport à une attente.

NOTE 2 Les objectifs peuvent avoir différents aspects (par exemple buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier).

NOTE 3 Un risque est souvent caractérisé en référence à des **événements** (2.17) et des **conséquences** (2.18) potentiels ou à une combinaison des deux.

NOTE 4 Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa **vraisemblance** (2.19).

NOTE 5 L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

[ISO Guide 73:2009, définition 1.1]

2.2
management du risque
activités coordonnées dans le but de diriger et piloter un organisme vis-à-vis du **risque** (2.1)

[ISO Guide 73:2009, définition 2.1]

2.3
cadre organisationnel de management du risque
ensemble d'éléments établissant les fondements et dispositions organisationnelles présidant à la conception, la mise en œuvre, la **surveillance** (2.28), la revue et l'amélioration continue du **management du risque** (2.2) dans tout l'organisme

NOTE 1 Les fondements incluent la politique, les objectifs, le mandat et l'engagement envers le management du **risque** (2.1).

NOTE 2 Les dispositions organisationnelles incluent les plans, les relations, les responsabilités, les ressources, les processus et les activités.

NOTE 3 Le cadre organisationnel du management du risque fait partie intégrante des politiques stratégiques et opérationnelles ainsi que des pratiques de l'ensemble de l'organisme.

[ISO Guide 73:2009, définition 2.1.1]

2.4
politique de management du risque
déclaration des intentions et des orientations générales d'un organisme en relation avec le **management du risque** (2.2)

[ISO Guide 73:2009, définition 2.1.2]

2.5
attitude face au risque
approche d'un organisme pour apprécier un **risque** (2.1) avant, éventuellement, de saisir ou préserver une opportunité ou de prendre ou rejeter un risque

[ISO Guide 73:2009, définition 3.7.1.1]

2.6
plan de management du risque
programme inclus dans le **cadre organisationnel de management du risque** (2.3), spécifiant l'approche, les composantes du management et les ressources auxquelles doit avoir recours le management du **risque** (2.1)

NOTE 1 Les composantes du management incluent, par exemple, les procédures, les pratiques, l'attribution des responsabilités, le déroulement chronologique des activités.

NOTE 2 Le plan de management du risque peut être appliqué à un produit, un processus, un projet particulier, à une partie de l'organisme ou à l'organisme tout entier.

[ISO Guide 73:2009, définition 2.1.3]

2.7
propriétaire du risque
personne ou entité ayant la responsabilité du **risque** (2.1) et ayant autorité pour le gérer

[ISO Guide 73:2009, définition 3.5.1.5]

2.8
processus de management du risque
application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de **surveillance** (2.28) et de revue des **risques** (2.1)

[ISO Guide 73:2009, définition 3.1]

2.9
établissement du contexte
définition des paramètres externes et internes à prendre en compte lors du management du risque et définition du domaine d'application ainsi que des **critères de risque** (2.22) pour la **politique de management du risque** (2.4)

[ISO Guide 73:2009, définition 3.3.1]

2.10
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses objectifs

NOTE Le contexte externe peut inclure

— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,

— les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme, et

— les relations avec les **parties prenantes** (2.13) externes, leurs perceptions et leurs valeurs.

[ISO Guide 73:2009, définition 3.3.1.1]

2.11
contexte interne
environnement interne dans lequel l'organisme cherche à atteindre ses objectifs

NOTE Le contexte interne peut inclure

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

— les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers,

— les capacités, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies),

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels),

— les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs,

— la culture de l'organisme,

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

— la forme et l'étendue des relations contractuelles.

[ISO Guide 73:2009, définition 3.3.1.2]

2.12
communication et concertation
processus itératifs et continus mis en œuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les **parties prenantes** (2.13) et autres parties, concernant le management du **risque** (2.1)

NOTE 1 Ces informations peuvent concerner l'existence, la nature, la forme, la **vraisemblance** (2.19), l'importance, l'évaluation, l'acceptabilité et le traitement du management du risque.

NOTE 2 La concertation est un processus de communication argumentée à double sens entre un organisme et ses parties prenantes sur une question donnée avant de prendre une décision ou de déterminer une orientation concernant ladite question. La concertation est

— un processus dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir, et

— une contribution à une prise de décision, et non une prise de décision conjointe.

[ISO Guide 73:2009, définition 3.2.1]

2.13
partie prenante
personne ou organisme susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

NOTE Un décideur peut être une partie prenante.

[ISO Guide 73:2009, définition 3.2.1.1]

2.14
appréciation du risque
ensemble du processus d'**identification des risques** (2.15), d'**analyse du risque** (2.21) et d'**évaluation du risque** (2.24)

[ISO Guide 73:2009, définition 3.4.1]

2.15
identification des risques
processus de recherche, de reconnaissance et de description des **risques** (2.1)

NOTE 1 L'identification des risques comprend l'identification des **sources de risque** (2.16), des **événements** (2.17), de leurs causes et de leurs **conséquences** (2.18) potentielles.

NOTE 2 L'identification des risques peut faire appel à des données historiques, des analyses théoriques, des avis d'experts et autres personnes compétentes et tenir compte des besoins des **parties prenantes** (2.13).

[ISO Guide 73:2009, définition 3.5.1]

2.16
source de risque
tout élément qui, seul ou combiné à d'autres, présente un potentiel intrinsèque d'engendrer un **risque** (2.1)

NOTE Une source de risque peut être tangible ou intangible.

[ISO Guide 73:2009, définition 3.5.1.2]

2.17
événement
occurrence ou changement d'un ensemble particulier de circonstances

NOTE 1 Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.

NOTE 2 Un événement peut consister en quelque chose qui ne se produit pas.

NOTE 3 Un événement peut parfois être qualifié «d'incident» ou «d'accident».

NOTE 4 Un événement sans **conséquences** (2.18) peut également être appelé «quasi-accident» ou «incident» ou «presque succès».

[ISO Guide 73:2009, définition 3.5.1.3]

2.18
conséquence
effet d'un **événement** (2.17) affectant les objectifs

NOTE 1 Un événement peut engendrer une série de conséquences.

NOTE 2 Une conséquence peut être certaine ou incertaine et peut avoir des effets positifs ou négatifs sur l'atteinte des objectifs.

NOTE 3 Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

NOTE 4 Des conséquences initiales peuvent déclencher des réactions en chaîne.

[ISO Guide 73:2009, définition 3.6.1.3]

2.19
vraisemblance
possibilité que quelque chose se produise

NOTE 1 Dans la terminologie du management du risque, 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 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.

[ISO Guide 73:2009, définition 3.6.1.1]

2.20
profil de risque
description d'un ensemble quelconque de **risques** (2.1)

NOTE Cet ensemble de risques peut inclure les risques relatifs à l'ensemble de l'organisme, à une partie de celui-ci, ou être défini autrement.

[ISO Guide 73:2009, définition 3.8.2.5]

2.21
analyse du risque
processus mis en œuvre pour comprendre la nature d'un **risque** (2.1) et pour déterminer le **niveau de risque** (2.23)

NOTE 1 L'analyse du risque fournit la base de l'**évaluation du risque** (2.24) et les décisions relatives au **traitement du risque** (2.25).

NOTE 2 L'analyse du risque inclut l'estimation du risque.

[ISO Guide 73:2009, définition 3.6.1]

2.22
critères de risque
termes de référence vis-à-vis desquels l'importance d'un **risque** (2.1) est évaluée

NOTE 1 Les critères de risque sont fondés sur les objectifs de l'organisme ainsi que sur le **contexte externe** (2.10) et **interne** (2.11).

NOTE 2 Les critères de risque peuvent être issus de normes, de lois, de politiques et d'autres exigences.

[ISO Guide 73:2009, définition 3.3.1.3]

2.23
niveau de risque
importance d'un **risque** (2.1) ou combinaison de risques, exprimée en termes de combinaison des **conséquences** (2.18) et de leur **vraisemblance** (2.19)

[ISO Guide 73:2009, définition 3.6.1.8]

2.24
évaluation du risque
processus de comparaison des résultats de l'**analyse du risque** (2.21) avec les **critères de risque** (2.22) afin de déterminer si le **risque** (2.1) et/ou son importance sont acceptables ou tolérables

NOTE L'évaluation du risque aide à la prise de décision relative au **traitement du risque** (2.25).

[ISO Guide 73:2009, définition 3.7.1]

2.25
traitement du risque
processus destiné à modifier un **risque** (2.1)

NOTE 1 Le traitement du risque peut inclure

— un refus du risque en décidant de ne pas démarrer 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** (2.16),

— une modification de la **vraisemblance** (2.19),

— une modification des **conséquences** (2.18),

— un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque), et

— un maintien du risque fondé sur une décision argumentée.

NOTE 2 Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

NOTE 3 Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

[ISO Guide 73:2009, définition 3.8.1]

2.26
moyen de maîtrise
mesure qui modifie un **risque** (2.1)

NOTE 1 Un moyen de maîtrise du risque inclut n'importe quels processus, politique, dispositif, pratique ou autres actions qui modifient un risque.

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

[ISO Guide 73:2009, définition 3.8.1.1]

2.27
risque résiduel
risque (2.1) subsistant après le **traitement du risque** (2.25)

NOTE 1 Un risque résiduel peut inclure un risque non identifié.

NOTE 2 Un risque résiduel peut également être appelé «risque pris».

[ISO Guide 73:2009, définition 3.8.1.6]

2.28
surveillance
vérification, supervision, observation critique ou détermination de l'état afin d'identifier continûment des changements par rapport au niveau de performance exigé ou attendu

NOTE La surveillance peut s'appliquer à un **cadre organisationnel de management du risque** (2.3), un **processus de management du risque** (2.8), un **risque** (2.1) ou un **moyen de maîtrise** (2.26) du risque.

[ISO Guide 73:2009, définition 3.8.2.1]

2.29
revue
activité entreprise afin de déterminer l'adaptation, l'adéquation et l'efficacité de l'objet étudié pour atteindre les objectifs établis

NOTE La revue peut s'appliquer à un **cadre organisationnel de management du risque** (2.3), un **processus de management du risque** (2.8), un **risque** (2.1) ou un **moyen de maîtrise** (2.26) du risque.

[ISO Guide 73:2009, définition 3.8.2.2]

3 Principes

Pour avoir un management des risques efficace, il convient qu'un organisme respecte, à tous les niveaux, les principes énoncés ci-dessous.

a) **Le management du risque crée de la valeur et la préserve.**

Le management du risque contribue de façon tangible à l'atteinte des objectifs et à l'amélioration des performances, par exemple dans le domaine de la santé et de la sécurité des personnes et des biens, de la conformité aux exigences légales et réglementaires, de l'acceptation par le public, de la protection de l'environnement, de la qualité des produits, du management de projets, de l'efficacité opérationnelle et de la gouvernance de l'organisme, ainsi que de sa réputation.

b) **Le management du risque est intégré aux processus organisationnels.**

Le management du risque n'est pas une activité indépendante séparée des principales activités et principaux processus de l'organisme. Le management du risque relève de la responsabilité de la direction et fait partie intégrante des processus organisationnels, dont la planification stratégique et tous les processus de management des projets et du changement.

c) **Le management du risque est intégré au processus de prise de décision.**

Le management du risque aide les décideurs à faire des choix argumentés, à définir des priorités d'actions et à choisir entre différents plans d'action.

d) **Le management du risque traite explicitement de l'incertitude.**

Le management du risque tient compte, de manière explicite, des incertitudes, de la nature de ces incertitudes, et de la façon dont elles peuvent être traitées.

e) **Le management du risque est systématique, structuré et utilisé en temps utile.**

Une approche systématique, en temps utile et structurée du management du risque contribue à l'efficacité de la démarche et à la cohérence de résultats comparables et fiables.

f) **Le management du risque s'appuie sur la meilleure information disponible.**

Les données d'entrée du processus de management du risque reposent sur des sources d'information, comme des données historiques, l'expérience, les retours d'information des parties prenantes, les observations, les prévisions et les avis d'experts. Toutefois, il convient que les décideurs s'informent et tiennent compte des éventuelles limites des données ou modèles utilisés, ainsi que des éventuelles divergences entre experts.

g) **Le management du risque est adapté.**

Le management du risque s'aligne sur le contexte externe et interne de l'organisme et son profil de risque.

h) **Le management du risque intègre les facteurs humains et culturels.**

Le management du risque permet d'identifier les aptitudes, les perceptions et les intentions des personnes externes et internes susceptibles de faciliter ou de gêner l'atteinte des objectifs de l'organisme.

i) **Le management du risque est transparent et participatif.**

L'implication appropriée et en temps voulu des parties prenantes, et notamment des décideurs à tous les niveaux de l'organisme, garantit que le management du risque reste pertinent et actuel. Elle permet également aux parties prenantes d'être correctement représentées et de voir leur opinion prise en compte dans la détermination des critères de risque.

j) **Le management du risque est dynamique, itératif et réactif au changement.**

Le management du risque perçoit continuellement les changements et y répond. Des événements internes et externes peuvent survenir, le contexte ou les connaissances peuvent changer, la surveillance et la revue des risques peuvent se mettre en place, alors de nouveaux risques peuvent surgir, certains être modifiés, tandis que d'autres disparaissent.

k) **Le management du risque facilite l'amélioration continue de l'organisme.**

Il convient que les organismes élaborent et mettent en œuvre des stratégies visant à améliorer leur maturité en matière de management du risque, comme pour tous les autres aspects de leur organisation.

L'Annexe A apporte des conseils supplémentaires pour les organismes souhaitant gérer plus efficacement le risque.

4 Cadre organisationnel

4.1 Généralités

Le succès du management du risque va dépendre de l'efficacité du cadre organisationnel de management qui fournit les bases et les dispositions permettant son intégration à tous les niveaux de l'organisme. Ce cadre organisationnel facilite un management efficace des risques dans tout le processus de management du risque (voir Article 5) à différents niveaux et dans des contextes spécifiques à l'organisme. Ce cadre garantit que les informations sur les risques émanant de ces processus du management du risque sont correctement rapportées et servent de base aux prises de décisions et à la responsabilisation de tous les niveaux concernés au sein de l'organisme.

Cet article décrit les composantes nécessaires au cadre organisationnel de management du risque et la façon dont elles interagissent de façon itérative, comme le montre la Figure 2.

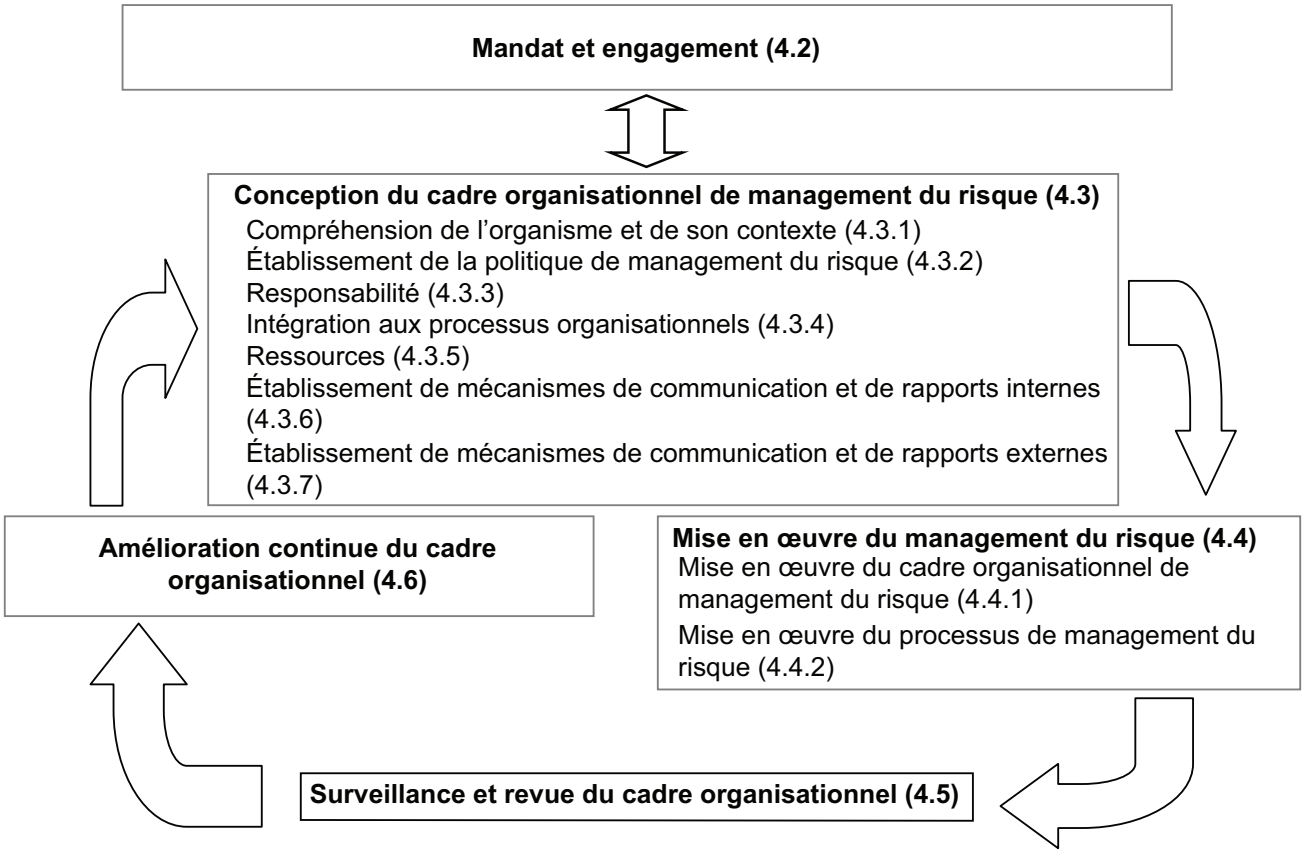

Figure 2 — Relations entre les composantes du cadre organisationnel de management du risque

Ce cadre n'est pas destiné à prescrire un système de management, mais plutôt à aider l'organisme à intégrer le management du risque dans son système de management global. Il convient donc que les organismes adaptent les composantes de ce cadre organisationnel à leurs besoins particuliers.

Si les pratiques et processus de management existant au sein d'un organisme comportent des composantes du management du risque ou si l'organisme a déjà adopté un processus de management du risque formalisé pour des types de situations ou de risques particuliers, il convient alors que ceux-ci soient revus de façon approfondie et appréciés à la lumière de la présente Norme internationale, en y incluant les attributs figurant dans l'Annexe A, afin de déterminer leur adéquation et leur efficacité.

4.2 Mandat et engagement

L'introduction du management du risque et l'assurance de son efficacité permanente exigent un engagement fort et durable de la direction de l'organisme, ainsi que l'établissement d'un plan stratégique rigoureux pour conduire à un engagement à tous les niveaux. Il convient que la direction

— définisse et approuve la politique de management du risque,

— s'assure que la culture de l'organisme et sa politique de management du risque sont en phase,

— détermine des indicateurs de performance du management du risque cohérents avec les indicateurs de performance de l'organisme,

— aligne les objectifs du management du risque sur les objectifs et stratégies de l'organisme,

— s'assure de la conformité légale et réglementaire,

— affecte les responsabilités aux niveaux appropriés de l'organisme,

— s'assure que les ressources nécessaires sont allouées au management du risque,

— communique les avantages du management du risque à l'ensemble des parties prenantes, et

— s'assure que le cadre organisationnel de management du risque reste approprié.

4.3 Conception du cadre organisationnel de management du risque

4.3.1 Compréhension de l'organisme et de son contexte

Préalablement à la conception et à la mise en œuvre du cadre organisationnel de management du risque, il est important d'évaluer et de comprendre le contexte tant interne qu'externe de l'organisme, étant donné que celui-ci peut influencer la conception du cadre organisationnel de façon significative.

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

a) l'environnement social et culturel, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,

b) les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme, et

c) les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

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

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

— les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers,

— les aptitudes, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies),

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels),

— les relations avec les parties prenantes internes, leurs perceptions et leurs valeurs,

— la culture de l'organisme,

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

— la forme et l'étendue des relations contractuelles.

4.3.2 Établissement de la politique de management du risque

Il convient que la politique de management du risque précise les objectifs et l'engagement de l'organisme en matière de management du risque et typiquement aborde les points suivants:

— les motivations de l'organisme en matière de management du risque;

— les liens entre les objectifs et autres politiques de l'organisme et sa politique de management du risque;

— les responsabilités en matière de management du risque;

— la manière dont les conflits d'intérêts sont traités;

— l'engagement de mettre les ressources nécessaires à la disposition des personnes responsables du management du risque;

— la manière dont les performances du management du risque vont être mesurées et rapportées;

— l'engagement à revoir et à améliorer la politique et le cadre organisationnel de management du risque périodiquement et à la suite d'un événement ou d'un changement de circonstances.

Il convient de communiquer de manière appropriée sur la politique de management du risque.

4.3.3 Responsabilité

Il convient que l'organisme s'assure que sont établies les responsabilités, l'autorité et les compétences appropriées en matière de management du risque, y compris concernant la mise en œuvre et la mise à jour du processus de management du risque, et qu'il s'assure de l'adéquation, de l'efficacité et de la performance de tous moyens de maîtrise du risque. Cela peut être facilité par

— l'identification des propriétaires du risque qui ont la responsabilité du risque et l'autorité pour le gérer,

— l'identification des responsables de l'élaboration, de la mise en œuvre et de la tenue à jour du cadre organisationnel de management du risque,

— l'identification des autres responsabilités à tous les niveaux de l'organisme en matière de processus de management du risque,

— la définition de mesures de performance et de processus internes et/ou externes de rapports et de transmission à un niveau supérieur, et

— l'établissement de niveaux de reconnaissance appropriés.

4.3.4 Intégration aux processus organisationnels

Il convient que le management du risque soit intégré à toutes les pratiques et tous les processus de l'organisme de façon à être pertinent, efficace et performant. Il convient que le processus de management du risque fasse partie intégrante et ne soit pas séparé de ces processus organisationnels. Il convient notamment que le management du risque soit pris en compte dans l'élaboration de la politique, les plans d'activité et stratégiques et leur revue, et dans les processus de management du changement.

Il convient d'élaborer un plan de management du risque à l'échelle de l'organisme afin de s'assurer que la politique de management du risque est mise en œuvre et que le management du risque est intégré à l'ensemble des pratiques et des processus de l'organisme. Le plan de management du risque peut être intégré à d'autres plans organisationnels, comme un plan stratégique.

4.3.5 Ressources

Il convient que l'organisme alloue les ressources nécessaires au management du risque.

Il convient que soient pris en compte

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

— les ressources nécessaires à chaque étape du processus de management du risque,

— les processus de l'organisme, les 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, et

— les programmes de formation.

4.3.6 Établissement de mécanismes de communication et de rapports internes

Il convient que l'organisme mette en place des mécanismes de communication et de rapports internes pour soutenir et encourager les responsabilités et l'appropriation du risque. Il convient que ces mécanismes garantissent

— la communication appropriée des principales composantes du cadre organisationnel de management du risque, et de toutes modifications ultérieures,

— l'existence de rapports internes appropriés sur le cadre organisationnel de management du risque, son efficacité et ses effets,

— la disponibilité des informations pertinentes issues de l'application du management du risque aux niveaux et aux moments appropriés, et

— l'existence de processus de concertation avec des parties prenantes internes.

Il convient que ces mécanismes comportent, le cas échéant, des processus permettant de rassembler les informations relatives au risque provenant de différentes sources, et peuvent avoir besoin de considérer la sensibilité de l'information.

4.3.7 Établissement de mécanismes de communication et de rapports externes

Il convient que l'organisme élabore et mette en œuvre un plan sur la façon de communiquer avec les parties prenantes externes. Il convient que cela implique

— la participation des parties prenantes externes appropriées et l'assurance d'un échange efficace d'informations,

— l'établissement de rapports externes conformes aux obligations légales, réglementaires et aux exigences de la gouvernance de l'organisme,

— la mise en place d'un retour d'information et de rapports sur la communication et la concertation,

— l'utilisation de la communication pour renforcer la confiance dans l'organisme, et

— la communication avec les parties prenantes en cas de crise ou d'imprévu.

Il convient que ces mécanismes comportent, le cas échéant, des processus permettant de rassembler les informations relatives au risque provenant de différentes sources, et peuvent avoir besoin de considérer la sensibilité de l'information.

4.4 Mise en œuvre du management du risque

4.4.1 Mise en œuvre du cadre organisationnel de management du risque

Pour la mise en œuvre du cadre organisationnel de management du risque, il convient que l'organisme

— définisse un calendrier et une stratégie appropriés pour la mise en œuvre du cadre organisationnel de management du risque,

— applique la politique et le processus de management du risque aux processus organisationnels,

— se conforme aux obligations légales et réglementaires,

— s'assure que les prises de décision, y compris l'élaboration et la détermination des objectifs, sont cohérentes avec les conclusions des processus de management du risque,

— organise des séances d'information et de formation, et

— communique et se concerte avec les parties prenantes afin de s'assurer que son cadre organisationnel de management du risque reste approprié.

4.4.2 Mise en œuvre du processus de management du risque

Il convient que le management du risque soit mis en œuvre en s'assurant que le processus de management du risque décrit dans l'Article 5 est appliqué dans le cadre d'un plan de management du risque, à toutes les fonctions et à tous les niveaux pertinents de l'organisme dans le cadre de ses pratiques et processus.

4.5 Surveillance et revue du cadre organisationnel

Afin de s'assurer que le management du risque est efficace et contribue à l'atteinte des performances organisationnelles, il convient que l'organisme

— mesure les performances de management du risque par rapport à des indicateurs dont la pertinence est revue périodiquement,

— mesure périodiquement les progrès et les écarts par rapport au plan de management du risque,

— examine périodiquement si le cadre organisationnel, la politique et le plan de management du risque sont toujours appropriés au vu du contexte interne et externe de l'organisme,

— établisse des rapports sur les risques, sur les avancées du plan de management du risque, et sur la façon dont la politique de management du risque est suivie, et

— vérifie l'efficacité du cadre organisationnel de management du risque.

4.6 Amélioration continue du cadre organisationnel

Sur la base des résultats de cette surveillance et de ces revues, il convient de prendre des décisions sur les possibilités d'amélioration du cadre organisationnel, de la politique et du plan de management du risque. Il convient que ces décisions entraînent des améliorations du management du risque et de la culture du management du risque de l'organisme.

5 Processus

5.1 Généralités

Il convient que le management du risque soit

— partie intégrante du management,

— intégré à la culture et aux pratiques, et

— adapté aux processus métiers de l'organisme.

Cela comprend les activités décrites de 5.2 à 5.6. Le processus de management du risque est présenté à la Figure 3.

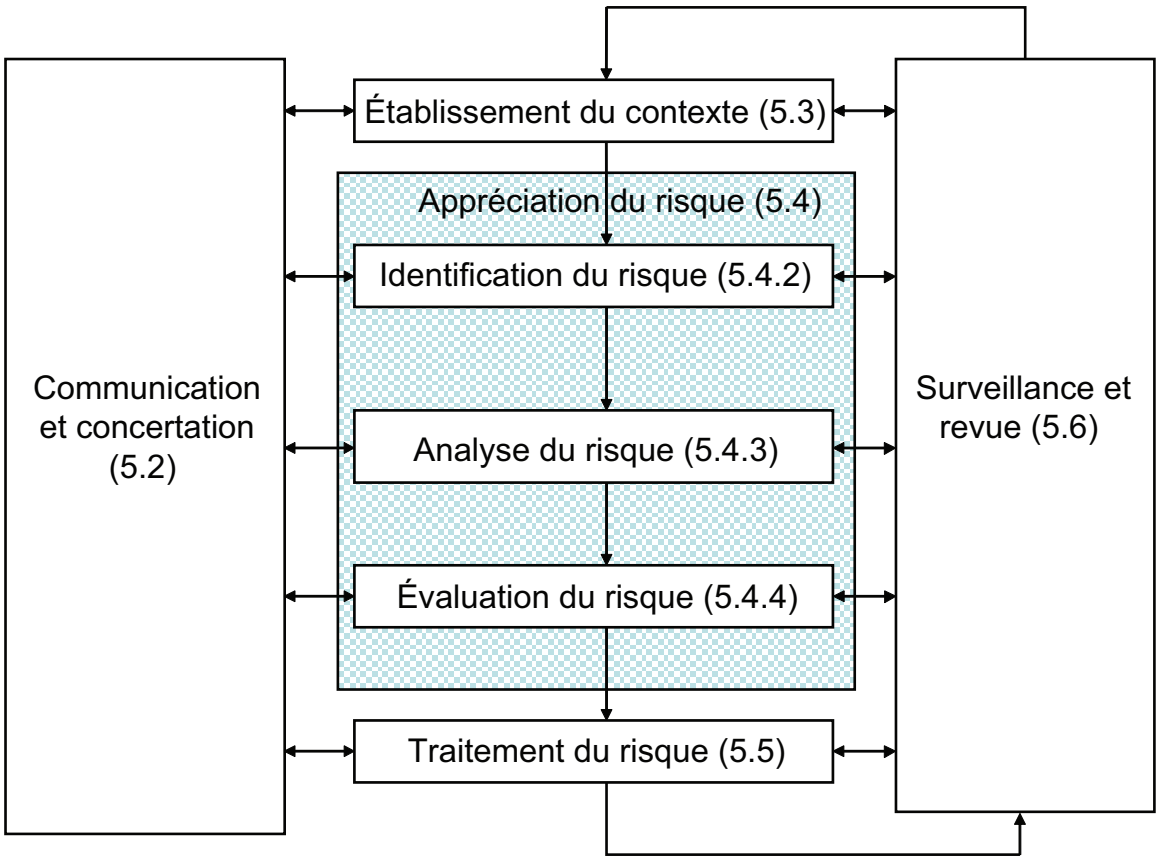

Figure 3 — Processus de management du risque

5.2 Communication et concertation

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

Il convient, par conséquent, d'élaborer des plans de communication et de concertation très tôt. Il convient que ces plans traitent des questions relatives au risque lui-même, à ses causes, à ses conséquences (si elles sont connues), et aux mesures prises pour le traiter. Il convient que l'efficacité de la communication et de la concertation internes et externes permette de s'assurer que les parties prenantes et les personnes responsables de la mise en œuvre du processus de management du risque comprennent les principes de prise de décisions et les raisons pour lesquelles certaines actions sont nécessaires.

Une approche consultative en équipe peut

— aider à définir correctement le contexte,

— s'assurer que les intérêts des parties prenantes sont compris et pris en considération,

— s'assurer que les risques sont correctement identifiés,

— réunir différents domaines d'expertise pour l'analyse des risques,

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

— conforter l'adhésion et le soutien à un plan de traitement,

— favoriser un management judicieux du changement au cours du processus de management du risque, et

— élaborer un plan de communication et de concertation interne et externe approprié.

La communication et la concertation avec les parties prenantes sont importantes car leur jugement sur le risque se fonde sur leur propre perception du risque. Ces perceptions du risque peuvent varier selon les différentes valeurs, les besoins, les hypothèses, les concepts et les préoccupations des parties prenantes. Leur opinion pouvant avoir un impact significatif sur les décisions prises, il convient que la perception des parties prenantes soit identifiée, enregistrée et prise en compte dans le processus de prise de décision.

Il convient que la communication et la concertation facilitent des échanges d'informations francs, pertinents, précis et compréhensibles, tenant compte de leur confidentialité et de l'intégrité personnelle.

5.3 Établissement du contexte

5.3.1 Généralités

En établissant le contexte, l'organisme énonce clairement ses objectifs, définit les paramètres internes et externes à prendre en compte dans le management du risque, et détermine le domaine d'application et les critères de risque pour la suite du processus. Bien que la plupart de ces paramètres soient semblables à ceux pris en compte dans la conception du cadre organisationnel de management du risque (voir 4.3.1) pour l'établissement du contexte du processus de management du risque, ils doivent être examinés en détail, notamment en ce qui concerne la façon dont ils se rattachent au domaine d'application du processus spécifique de management du risque.

5.3.2 Établissement du contexte externe

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

Il est important de comprendre le contexte externe afin de s'assurer que les objectifs et les préoccupations des parties prenantes externes sont pris en compte lors de l'élaboration des critères de risque. Le contexte externe est basé sur le contexte à l'échelle de l'organisme, avec toutefois des détails spécifiques découlant des obligations légales et réglementaires, des perceptions des parties prenantes et d'autres aspects des risques propres au domaine d'application du processus de management du risque.

Le contexte externe peut inclure, sans que la liste soit exhaustive,

— l'environnement social et culturel, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local,

— les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme, et

— les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

5.3.3 Établissement du contexte interne

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

Il convient que le processus de management du risque soit cohérent avec la culture, les processus, la structure et la stratégie de l'organisme. Le contexte interne comprend tout ce qui, au sein d'un organisme, peut influencer la manière dont l'organisme gère le risque. Il convient de l'établir car

a) le management du risque se fait dans le contexte des objectifs de l'organisme,

b) il convient d'envisager les objectifs et les critères d'un projet, d'un processus ou d'une activité spécifique à la lumière des objectifs de l'organisme dans leur ensemble, et

c) certains organismes ne parviennent pas à identifier les opportunités leur permettant d'atteindre leurs objectifs en matière de stratégie, de projet ou d'activité, ce qui compromet la continuité de l'engagement, de la crédibilité, de la confiance et des valeurs de l'organisme.

Il est nécessaire de comprendre le contexte interne. Cela peut inclure, sans toutefois s'y limiter

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

— les politiques, les objectifs et les stratégies mises en place pour les atteindre,

— les aptitudes, en termes de ressources et de connaissances (par exemple capital, temps, personnels, processus, systèmes et technologies),

— les relations avec les parties prenantes internes, leurs perceptions et leurs valeurs,

— la culture de l'organisme,

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels),

— les normes, principes directeurs et modèles adoptés par l'organisme, et

— la forme et l'étendue des relations contractuelles.

5.3.4 Établissement du contexte du processus de management du risque

Il convient de fixer les objectifs, les stratégies, les domaines d'application et les paramètres des activités de l'organisme ou des parties de l'organisme où le processus de management du risque s'applique. Il convient d'entreprendre le management du risque en tenant compte de la nécessité de justifier les ressources servant à sa mise en œuvre. Il convient également de spécifier les ressources nécessaires, les responsabilités et autorités ainsi que les enregistrements à conserver.

Le contexte du processus de management du risque varie selon les besoins de l'organisme. Il peut inclure, sans toutefois s'y limiter

— la définition des buts et des objectifs des activités de management du risque,

— la définition des responsabilités relatives au processus de management du risque,

— la définition du domaine d'application ainsi que le degré et l'étendue des activités de management du risque à entreprendre, y compris ce qui est spécifiquement inclus et exclu,

— la définition de l'activité, du processus, de la fonction, du projet, du produit, du service ou de l'actif en termes de temps et de lieu,

— la définition des relations entre un projet, un processus ou une activité donné et les autres projets, processus ou activités de l'organisme,

— la définition des méthodes d'appréciation du risque,

— la définition de la méthode selon laquelle les performances et de l'efficacité du management du risque sont évaluées,

— l'identification et la spécification des décisions à prendre, et

— l'identification, le domaine d'application ou le cadre organisationnel des études requises, leur étendue et leurs objectifs, ainsi que les ressources nécessaires à leur réalisation.

Il convient que la prise en compte de ces facteurs et des autres facteurs pertinents permette de s'assurer que l'approche de management du risque retenue est adaptée aux circonstances, à l'organisme et aux risques affectant l'atteinte de ses objectifs.

5.3.5 Définition des critères de risque

Il convient que l'organisme définisse des critères permettant d'évaluer l'importance du risque. Il convient que ces critères reflètent les valeurs, les objectifs et les ressources de l'organisme. Certains critères peuvent être imposés ou résulter d'obligations légales et réglementaires, ou d'autres exigences auxquelles l'organisme répond. Il convient que les critères de risque soient cohérents avec la politique de management du risque de l'organisme (voir 4.3.2), soient définis au début de tout processus de management du risque et soient revus continuellement.

Lors de la définition des critères de risque, il convient de tenir compte, entre autres, des facteurs suivants:

— la nature et les types de causes et de conséquences qui peuvent survenir, et la façon dont elles vont être mesurées;

— la méthode de définition de la vraisemblance;

— l'échelle de la vraisemblance et/ou de la (des) conséquence(s);

— la méthode de détermination du niveau de risque;

— les avis des parties prenantes;

— le niveau à partir duquel le risque devient acceptable ou tolérable; et

— la prise en compte ou non des combinaisons de plusieurs risques et, le cas échéant, la méthode à utiliser et les combinaisons à considérer.

5.4 Appréciation du risque

5.4.1 Généralités

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

NOTE L'ISO/CEI 31010 donne des lignes directrices sur les techniques d'appréciation du risque.

5.4.2 Identification du risque

Il convient que l'organisme identifie les sources de risque, les domaines d'impact, les événements (y compris les changements de circonstances), ainsi que leurs causes et conséquences potentielles. Cette étape a pour objectif de dresser une liste exhaustive des risques basée sur les événements susceptibles de provoquer, de stimuler, d'empêcher, de gêner, d'accélérer ou de retarder l'atteinte des objectifs. Il est important d'identifier les risques associés au fait de ne pas saisir une opportunité. Il est essentiel de procéder à une identification exhaustive, car un risque non identifié à ce stade ne sera pas inclus dans une analyse ultérieure.

Il convient que l'identification inclue les risques, que leur source soit ou non sous le contrôle de l'organisme, même si la source ou la cause du risque peut ne pas être évidente. Il convient que l'identification du risque comporte l'examen des réactions en chaîne des conséquences particulières, y compris les effets en cascade et cumulatifs. Il convient également d'examiner un large éventail de conséquences, même si la source ou la cause du risque peuvent ne pas être évidentes. Tout en identifiant ce qui peut se produire, il est nécessaire d'examiner les causes possibles et les scénarios des conséquences éventuelles. Il convient d'étudier toutes les causes et conséquences significatives.

Il convient que l'organisme utilise des outils et techniques d'identification des risques adaptés à ses objectifs et ses aptitudes, et aux risques auxquels il est exposé. Il est essentiel que les informations utilisées pour l'identification des risques soient pertinentes et à jour. Il convient autant que possible qu'elles soient accompagnées d'une documentation appropriée. Il convient que les personnes ayant les connaissances appropriées participent à l'identification des risques.

5.4.3 Analyse du risque

L'analyse du risque nécessite d'acquérir une compréhension du risque. L'analyse du risque fournit des données pour évaluer les risques et prendre la décision de les traiter ou non, et permet de choisir les stratégies et méthodes de traitement les plus appropriées. L'analyse du risque peut aussi contribuer à la prise de décisions quand il faut effectuer des choix et que les options impliquent différents types et niveaux de risque.

L'analyse du risque implique la prise en compte des causes et sources de risque, de leurs conséquences positives et négatives, et de la vraisemblance que ces conséquences surviennent. Il convient d'identifier les facteurs affectant les conséquences et leur vraisemblance. Le risque est analysé en déterminant les conséquences et leur vraisemblance, ainsi que d'autres attributs du risque. Un événement peut avoir des conséquences multiples et affecter des objectifs multiples. Il convient de prendre en compte les moyens de maîtrise des risques existants, leur efficacité et leur performance.

Il convient que la façon dont les conséquences et leur vraisemblance sont exprimées ainsi que la manière dont elles sont combinées afin de déterminer un niveau de risque correspondent au type de risque, aux informations disponibles et à l'objectif de l'appréciation du risque. Il convient de veiller à la cohérence avec les critères de risque. Il est également important de tenir compte de l'interdépendance des différents risques et de leurs sources.

Il convient que le degré de confiance dans la détermination du niveau du risque et de sa sensibilité à des conditions préalables et à des hypothèses soit pris en compte dans l'analyse et communiqué effectivement aux décideurs et, si nécessaire, aux autres parties prenantes. Il convient que les facteurs, comme une divergence d'opinions entre experts, une incertitude, la disponibilité, la qualité, la quantité et la validité de la pertinence des informations ou les limites des modélisations soient mentionnées, voire soulignées.

L'analyse du risque peut être menée à différents niveaux de détail en fonction du risque, de la finalité de l'analyse et des informations, des données et des ressources disponibles. L'analyse peut être qualitative, semi-quantitative, quantitative, ou une combinaison des trois, selon les circonstances.

Les conséquences et leur vraisemblance peuvent être déterminées en modélisant les suites d'un événement ou d'un ensemble d'événements, ou par extrapolation d'études expérimentales ou de données disponibles. Les conséquences peuvent être exprimées en termes d'impacts tangibles et intangibles. Dans certains cas, plusieurs valeurs numériques ou descripteurs sont nécessaires pour préciser les conséquences et leur vraisemblance à différents moments, en différents lieux, dans différents groupes ou situations.

5.4.4 Évaluation du risque

Sur la base des résultats de l'analyse du risque, le but de l'évaluation du risque est d'aider les décideurs à déterminer les risques nécessitant un traitement et la priorité dans la mise en œuvre des traitements.

L'évaluation du risque consiste à comparer le niveau de risque déterminé au cours du processus d'analyse aux critères de risque établis lors de l'établissement du contexte. Sur la base de cette comparaison, il est possible d'étudier la nécessité d'un traitement.

Il convient que les décisions tiennent compte du contexte élargi du risque et en particulier considèrent la tolérance au risque des parties autres que l'organisme qui tire avantage du risque. Il convient que les décisions respectent les obligations légales, réglementaires et autres exigences.

Dans certains cas, l'évaluation du risque peut déboucher sur la décision d'entreprendre une analyse plus approfondie. L'évaluation du risque peut également conduire à la décision de ne pas traiter le risque autrement qu'en maintenant les moyens de maîtrise du risque existants. Cette décision va dépendre de l'attitude de l'organisme face au risque, ainsi que des critères de risque qui ont été établis.

5.5 Traitement du risque

5.5.1 Généralités

Le traitement du risque implique le choix et la mise en œuvre d'une ou de plusieurs options de modification des risques. Une fois mis en œuvre, les traitements engendrent ou modifient les moyens de maîtrise du risque.

Le traitement du risque implique un processus itératif:

— évaluer un traitement du risque;

— décider si les niveaux de risque résiduels sont tolérables;

— s'ils ne sont pas tolérables, générer un nouveau traitement du risque; et

— apprécier l'efficacité de ce traitement.

Les options de traitement du risque ne s'excluent pas nécessairement les unes les autres, ni ne sont appropriées à toutes les circonstances. Ces options peuvent inclure

a) un refus du risque marqué par la décision de ne pas commencer ou poursuivre l'activité porteuse du risque,

b) la prise ou l'augmentation d'un risque afin de poursuivre une opportunité,

c) l'élimination de la source de risque,

d) une modification de la vraisemblance,

e) une modification des conséquences,

f) un partage du risque avec une autre ou d'autres parties (y compris les contrats et le financement du risque), et

g) un maintien du risque fondé sur un choix argumenté.

5.5.2 Sélection des options de traitement du risque

La sélection de l'option de traitement du risque la plus appropriée implique de comparer les coûts et les efforts de mise en œuvre par rapport aux avantages obtenus, compte tenu des obligations légales, réglementaires et autres exigences, comme la responsabilité sociale et la protection de l'environnement naturel. Il convient que les décisions tiennent aussi compte des risques dont le traitement n'est pas justifiable au plan économique, par exemple certains risques graves (conséquences hautement négatives) mais rares (faible vraisemblance).

Un certain nombre d'options de traitement peuvent être examinées et appliquées individuellement ou en combinaison. Normalement l'organisme peut tirer avantage de l'adoption d'une combinaison d'options de traitement.

Lors du choix des options de traitement du risque, il convient que l'organisme tienne compte des valeurs et des perceptions des parties prenantes et examine les moyens les plus appropriés de communiquer avec elles. Lorsque les options de traitement du risque peuvent avoir un impact n'importe où au sein de l'organisme ou chez les parties prenantes, il convient que celles-ci soient impliquées dans la décision. À efficacité égale, certains traitements du risque peuvent être plus acceptables que d'autres pour certaines parties prenantes.

Il convient que le plan de traitement identifie clairement l'ordre des priorités de mise en œuvre des traitements individuels du risque.

Le traitement lui-même peut engendrer des risques. La défaillance ou l'inefficacité des mesures de traitement envisagées peuvent constituer un risque significatif. Pour s'assurer que les mesures restent efficaces, la surveillance doit faire partie intégrante du plan de traitement du risque.

Le traitement du risque peut également engendrer des risques secondaires qui doivent être appréciés, traités, surveillés et revus. Il convient que ces risques secondaires soient intégrés au même plan de traitement que le risque original et ne soient pas traités en tant que nouveau risque. Il convient que le lien entre les deux risques soit identifié et fasse l'objet d'un suivi.

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

Les plans de traitement du risque sont destinés à documenter la manière dont les options de traitement choisies sont mises en œuvre. Il convient que les informations fournies dans ces plans de traitement comportent

— les raisons ayant motivé le choix des options de traitement, y compris les avantages attendus,

— les personnes responsables de l'approbation du plan et celles responsables de sa mise en œuvre,

— les actions proposées,

— les besoins en ressources, en tenant compte des impondérables,

— la mesure des performances et les contraintes,

— les exigences en matière de rapports et de surveillance, et

— le calendrier et le séquencement.

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

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 surveillance et revue et, le cas échéant, fasse l'objet d'un traitement supplémentaire.

5.6 Surveillance et revue

Il convient que la surveillance et la revue soient planifiées dans le processus de management du risque et s'accompagnent d'un contrôle ou d'une surveillance régulière. Ce contrôle ou cette surveillance peuvent être périodiques ou ponctuels.

Il convient que les responsabilités de surveillance et de revue soient clairement définies.

Il convient que les processus de surveillance et de revue de l'organisme s'appliquent à tous les aspects du processus de management du risque afin de pouvoir

— s'assurer que les moyens de maîtrise sont efficaces et performants aussi bien dans leur conception que dans leur utilisation,

— obtenir des informations supplémentaires pour améliorer l'appréciation du risque,

— analyser et tirer les leçons des événements (y compris des incidents), des changements, des tendances, des succès et des échecs,

— détecter les changements dans le contexte interne et externe, y compris les changements concernant les critères de risque et le risque lui-même qui peuvent nécessiter une révision des traitements du risque et des priorités, et

— identifier les risques émergents.

L'avancement de la mise en œuvre des plans de traitement des risques constitue une mesure de la performance. Les résultats peuvent être intégrés au management global des performances de l'organisme, à leur mesurage et aux activités d'élaboration de rapports externes et internes.

Il convient que les résultats de la surveillance et de la revue soient enregistrés, fassent l'objet de rapports internes et externes selon les besoins, et servent de données à la revue du cadre organisationnel de management du risque (voir 4.5).

5.7 Enregistrement du processus de management du risque

Il convient que les activités de management du risque puissent être tracées. Dans le processus de management du risque, les enregistrements fournissent la base de l'amélioration des méthodes et des outils ainsi que du processus dans son ensemble.

Il convient que les décisions relatives à la création des enregistrements prennent en compte

— les besoins de l'organisme en matière d'acquisition continue de connaissances,

— les avantages de la réutilisation d'informations pour répondre à des objectifs de management,

— les coûts et le travail liés à la création et à la maintenance des enregistrements,

— les nécessités légales, réglementaires et opérationnelles d'effectuer des enregistrements,

— la méthode d'accès, la facilité de consultation et les moyens de stockage,

— la période de conservation, et

— le caractère sensible des informations.

Annexe A
(informative)

Attributs d'un management du risque élevé

A.1 Généralités

Il convient que tous les organismes visent le niveau approprié de performance de leur cadre organisationnel de management du risque, en fonction du caractère critique des décisions à prendre. La liste des attributs ci-dessous représente un niveau de performance élevé dans le domaine du management du risque. Afin d'aider les organismes à mesurer leurs propres performances par rapport à ces critères, des indicateurs tangibles sont indiqués pour chaque attribut.

A.2 Points principaux

A.2.1 L'organisme a une compréhension totale, correcte et actualisée de ses risques.

A.2.2 Les risques de l'organisme entrent dans les limites des critères de risque.

A.3 Attributs

A.3.1 Amélioration continue

L'accent est mis sur l'amélioration continue du management du risque par la mise en place d'objectifs de performance organisationnelle, le mesurage, la revue et la modification induite des processus, les systèmes, les ressources, les aptitudes et les compétences.

Des indicateurs tangibles sont, par exemple, l'existence d'objectifs de performance explicites permettant de mesurer les performances de l'organisme et celles de ses responsables. Les performances de l'organisme peuvent être publiées et communiquées. Il est normalement procédé à au moins une revue annuelle des performances, puis à une révision des processus, et à la définition de nouveaux objectifs de performance pour la période suivante.

Cette évaluation des performances du management du risque fait partie intégrante du système global d'évaluation et de mesurage des performances des services et des personnes existant au sein de l'organisme.

A.3.2 Responsabilité complète des risques

Un management du risque développé inclut la responsabilité complète pleinement définie et acceptée des risques, des moyens de leur maîtrise et des tâches de traitement des risques. Les personnes désignées en acceptent la pleine responsabilité, ont les compétences nécessaires et disposent des ressources adaptées leur permettant de vérifier les moyen de maîtrise du risque, de surveiller les risques, d'améliorer les moyens de maîtrise du risque, et de communiquer efficacement sur les risques et leur management avec les parties prenantes internes et externes.

Des indicateurs tangibles sont, par exemple, le fait que tous les membres d'un organisme ont pleine conscience des risques, des moyens de maîtrise du risque et des tâches dont ils ont la responsabilité. Normalement, cela figure dans les descriptions de poste/de métier, les bases de données ou les systèmes d'information. Il convient que la définition des rôles et des responsabilités en matière de management du risque fasse partie des procédures d'accueil des nouveaux arrivants à un poste ou une fonction.

L'organisme s'assure que les personnes responsables sont en mesure de remplir ce rôle en leur fournissant l'autorité, le temps, la formation, les ressources et les compétences nécessaires pour assumer leurs responsabilités.

A.3.3 Application du management du risque dans toutes les prises de décision

Toutes les prises de décision au sein de l'organisme, quelles que soient leur importance et leur portée, impliquent la prise en compte explicite des risques et l'application du management du risque dans une mesure appropriée.

Des indicateurs tangibles sont, par exemple, l'existence d'enregistrements des réunions et des décisions montrant l'existence de discussions formelles sur les risques. En outre, il convient de pouvoir démontrer que toutes les composantes du management du risque sont représentées dans les processus clés de prise de décision de l'organisme, par exemple dans les décisions d'allocation du capital, de projets importants, de restructuration et de changements organisationnels. C'est pour ces raisons qu'un management du risque solidement ancré est considéré, au sein de l'organisme, comme la base d'une gouvernance efficace.

A.3.4 Communication continue

Un management du risque élevé dans le cadre d'une bonne gouvernance implique une communication continue avec les parties prenantes internes et externes, comprenant l'élaboration de rapports exhaustifs et fréquents sur les performances du management du risque.

La communication avec les parties prenantes en tant que composante entière et essentielle du management du risque est un exemple d'indicateur tangible. La communication est considérée à juste titre comme un processus allant dans les deux sens et permettant des prises de décisions argumentées sur le niveau de risque et la nécessité d'un traitement du risque en fonction de critères de risque exhaustifs et correctement établis.

Des rapports internes et externes exhaustifs et fréquents tant sur les risques significatifs que sur les performances du management du risque contribuent dans une large mesure à une gouvernance efficace au sein de l'organisme.

A.3.5 Intégration complète dans la structure de gouvernance de l'organisme

Le management du risque est considéré comme central dans les processus de management de l'organisme, de sorte que les risques sont envisagés en termes d'effet de l'incertitude sur l'atteinte des objectifs. La structure et le processus de gouvernance de l'organisme reposent sur le management du risque. Un management du risque efficace est considéré comme essentiel par les dirigeants pour l'atteinte des objectifs de l'organisme.

Des indicateurs tangibles sont, par exemple, des discours tenus par les dirigeants ainsi que des documents écrits importants de l'organisme qui utilisent le terme «incertitude» en rapport avec les risques. En général, cet attribut ressort également des déclarations de politique de l'organisme, notamment de celles concernant le management du risque. Normalement, cet attribut doit pouvoir se vérifier lors des entretiens avec les dirigeants et être prouvé par leurs actions et leurs déclarations.

Bibliographie

[1] ISO Guide 73:2009, *Management du risque — Vocabulaire*

[2] ISO/CEI 31010, *Gestion des risques — Techniques d'évaluation des risques*

