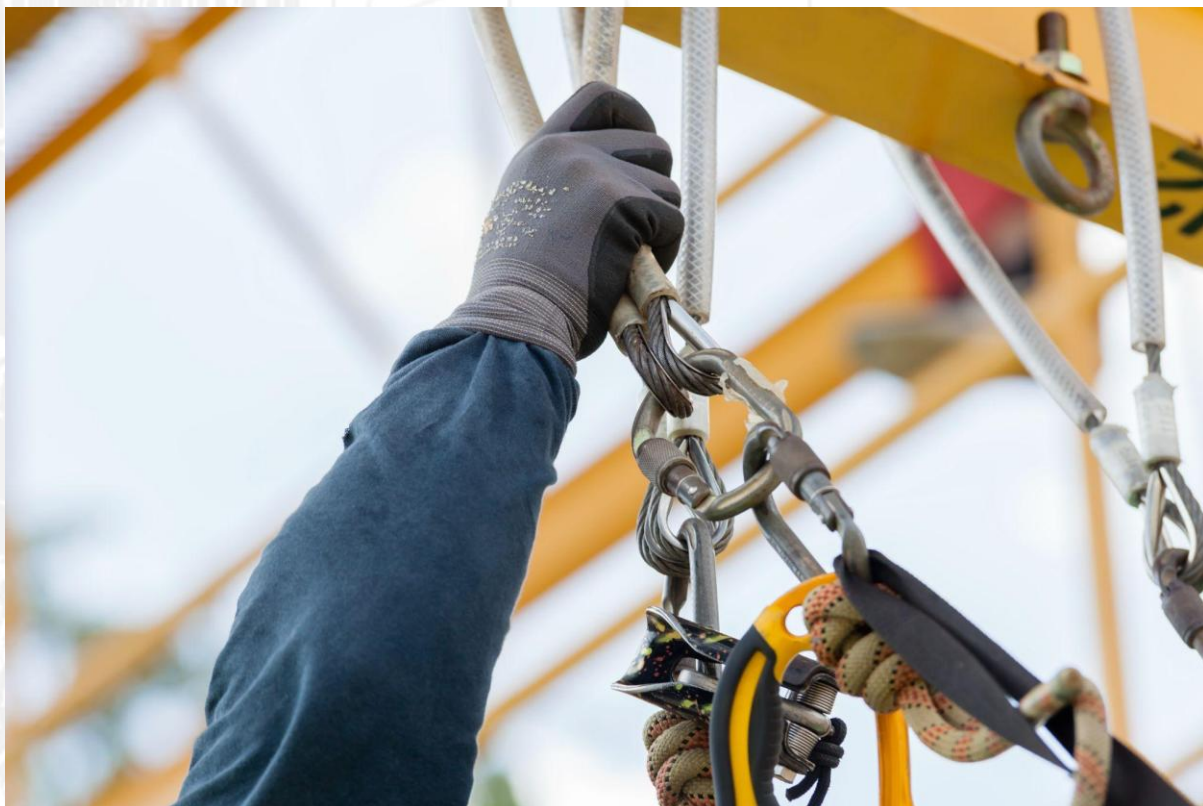


## MANAGEMENT DU RISQUE



La norme ISO 31000 « Management du risque – lignes directrices » est un guide de référence pour la gestion des risques en entreprise et pour type d'organisation publique ou privée, sans distinction de taille, d'activité ou de secteur.

Établie par l'Organisation internationale de normalisation (ISO), cette norme – permettant de gérer toute forme de risque – vise à préserver la valeur des organisations et à leur permettre de développer des stratégies éclairées pour améliorer leur performance.

L'émergence de nouveaux risques (réputation, cybercriminalité, terrorisme...) et l'évolution des pratiques dans la gestion du risque ont entraîné une évolution de cette norme. La dernière version de ce guide (ISO 31000:2018) souligne notamment la nécessité d'une implication de l'ensemble des acteurs de l'entreprise (et plus uniquement des professionnels de la gestion du risque).

Les principales modifications par rapport à la précédente édition (ISO 31000:2009) sont les suivantes :

- Revue des principes de management du risque
- Mise en avant du leadership de la direction et de l'intégration du management du risque
- Importance accrue accordée à la nature itérative du management du risque

- Simplification du contenu pour s'adapter à de multiples besoins et contextes

L'ISO 31000 définit les bases fondamentales du management du risque selon trois axes : les principes, le cadre organisationnel et le processus.

## Les principes

Les principes rassemblent les éléments caractéristiques d'un management du risque efficace. Ils permettent d'établir le cadre organisationnel et les processus, afin de gérer les effets de l'incertitude sur les objectifs de l'entreprise.

Le management du risque est intégré à toutes les activités de l'entreprise. Il nécessite une approche globale et structurée afin de permettre une mesure fiable des résultats.

L'ensemble des dispositions à l'œuvre dans le management du risque doit être adapté au contexte interne de l'organisation et à ses possibles influences externes, tout en restant en phase avec les objectifs de l'entreprise.

Le management du risque se doit d'être inclusif : l'implication des différents acteurs est décisive pour conduire des actions pertinentes et efficaces. Les facteurs humains et culturels sont eux aussi pris en compte dans ces principes.

Les risques n'étant pas figés une fois identifiés et traités, la conduite de la gestion des risques doit rester dynamique pour permettre à l'entreprise d'anticiper, de détecter, et de réagir au mieux à tout changement.

Les données utilisées dans la gestion des risques (historiques, actuelles et prévisionnelles) sont régulièrement actualisées, et rendues accessibles aux différentes parties prenantes afin qu'elles disposent de la meilleure information disponible dans le cadre de leurs actions quotidiennes.

Enfin, le management du risque suit évidemment un cycle d'amélioration continue. L'apprentissage et l'expérience viennent enrichir le dispositif de management du risque.

## Le cadre organisationnel

Le cadre organisationnel aide l'entreprise à intégrer le management du risque dans ses activités et ses fonctions significatives. Son efficacité en dépend, notamment dans la prise de décisions. Les fonctions dirigeantes de l'entreprise doivent donc être pleinement impliquées.

Le déploiement du cadre organisationnel réunit l'intégration, la conception, la mise en œuvre, l'évaluation et l'amélioration du management du risque au sein de l'entreprise.

La conception est la définition d'un cadre de fonctionnement apte à :

- Analyser le contexte interne (sens et valeurs de l'entreprise, stratégie, ressources...) et externe (facteurs sociaux, relations contractuelles, dépendances...)
- Définir l'engagement en matière de management du risque (culture d'entreprise, responsabilités, indicateurs de performance, ...)
- Attribuer des rôles et des responsabilités, et les communiquer en soulignant que le management du risque est une responsabilité fondamentale.
- Affecter les ressources nécessaires (personnels, systèmes de gestion, formation...)
- Consulter et communiquer avec les publics ciblés pour soutenir le cadre organisationnel

La mise en œuvre du cadre organisationnel intègre :

- L'élaboration d'un plan (calendrier, ressources)
- L'identification des chaînes de décision (où, quand, comment, par qui)
- La modification éventuelle de processus existants
- La vérification que l'ensemble des dispositions à l'œuvre est compris et appliqué

L'évaluation de l'efficacité du cadre organisationnel repose sur :

- La mesure de performance de ses indicateurs et des comportements attendus
- L'évaluation de la pertinence de son maintien « en l'état » vis-à-vis des objectifs

L'amélioration du cadre organisationnel implique que l'entreprise le contrôle de manière continue, afin de l'adapter aux changements qui ne manqueront pas de survenir.

## Le processus

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 et revue, d'enregistrement et de compte rendu du risque.

La communication et la consultation ont pour but d'aider les parties prenantes à comprendre le risque, les principes de prise de décisions et les raisons pour lesquelles certaines actions sont nécessaires. Ces deux activités réunissent différents domaines d'expertise et assurent la prise en compte d'une pluralité de points de vue. Par une étroite coordination, elles facilitent les échanges et mettent à disposition les informations nécessaires à la surveillance du risque et à la prise de décision.

La définition du périmètre d'application, du contexte et des critères a pour but d'adapter le processus de management du risque en permettant une appréciation efficace et un traitement approprié. Les éléments qui doivent être pris en compte relèvent notamment des objectifs à atteindre, des ressources et outils techniques nécessaires à l'appréciation du risque, et des interactions internes à l'organisation (qu'il soit question de projets, de processus ou d'activités).

Le contexte (interne et externe), c'est-à-dire l'environnement dans lequel évolue l'entreprise doit être abordé dans toutes ses dimensions, y compris dans les facteurs organisationnels qui peuvent être une source de risque.

## Critères de risque

En fonction de ses objectifs, l'entreprise doit définir le type de risques qui peuvent être pris ou non. Elle doit également définir les critères permettant d'en évaluer l'importance, et s'assurer que ces critères soient en cohérence - pour chacune de ses activités - avec ses valeurs, ses ressources et politiques en place en matière de management du risque.

Pour établir les critères de risques, ces éléments sont à prendre en considération :

- La nature et le type d'incertitudes pouvant avoir une incidence sur les résultats et les objectifs
- La façon dont sont définies et mesurées les conséquences et les vraisemblances de ces risques
- 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 sont prises en compte
- La capacité de l'entreprise

## L'appréciation du risque

L'appréciation du risque se définit comme le processus d'identification, d'analyse et d'évaluation du risque. Elle doit être menée de façon systématique, itérative et collaborative :

- L'identification du risque consiste à rechercher, reconnaître et décrire les risques qui peuvent aider ou empêcher l'entreprise d'atteindre ses objectifs. De nombreux facteurs et leurs relations sont à prendre en compte (causes et événements, menaces et opportunités, vulnérabilité et capacité, ...)
- L'analyse du risque a pour but de comprendre la nature du risque et ses caractéristiques. Elle inclut notamment des facteurs de vraisemblance d'événements et leurs conséquences, la nature et l'importance des conséquences, l'efficacité des moyens de maîtrise existants...
- L'évaluation du risque vise à comparer les résultats de l'analyse du risque aux critères de risque établis afin de déterminer si une action supplémentaire est exigée, permettant ainsi la prise de décision (exemples : maintenir les moyens existants, examiner les options de traitement, entreprendre une analyse plus approfondie)

## Traitement du risque

La phase de traitement a pour but d'établir les options à choisir pour réduire le risque et mettre en œuvre les actions pour y parvenir. Le traitement du risque implique aussi d'apprécier l'efficacité des actions menées, déterminer si le risque résiduel est acceptable ou non, et dans ce dernier cas, d'envisager un traitement complémentaire.

## Suivi et revue

Le suivi et la revue ont pour but l'amélioration de la qualité et de l'efficacité des solutions, de leur mise en œuvre et des résultats obtenus face au risque. Le suivi et la revue comprennent : la planification, le recueil et l'analyse d'informations, l'enregistrement des résultats et le retour d'information.

Le processus de management du risque et ses résultats sont documentés et font l'objet de rapports, afin de communiquer au sein de l'entreprise, fournir des informations pour la prise de décision, améliorer le management du risque, faciliter l'échange d'informations et l'interaction avec toutes les parties prenantes.

