

# Outil 6 : Exemple de liste de questions types liées à l'identification et l'évaluation des risques

Dans le cadre de sa mission de contrôle, le comité d'audit veillera à ce que les informations sur la gestion des risques lui soient transmises régulièrement.

Afin de s'acquitter des missions prévues dans le cadre de la charte, le comité d'audit doit déterminer s'il reçoit de manière suffisamment fréquente les informations pertinentes concernant la gestion des risques. Au moins une fois par an, il doit déterminer si les informations qui lui sont communiquées par la direction sont pertinentes et opportunes. Ces informations portent aussi bien sur des éléments financiers ou non financiers, actuels ou à venir. Le comité d'audit doit également s'entretenir avec la direction générale, ainsi qu'avec les responsables de l'audit interne et externe au sujet de la gestion des risques.

Le comité d'audit pourra s'appuyer sur les questions suivantes pour structurer les discussions avec la direction. Cette liste n'est pas exhaustive et nécessitera des adaptations en fonction des problématiques spécifiques de la société.

## Système de gestion des risques

## Evaluation du système de gestion des risques

### Stratégie en matière de risques :

Approche visant à identifier et gérer les risques, fondée sur les stratégies et les objectifs de l'entité.

- › Quels sont les risques inhérents à la stratégie et aux objectifs de l'activité ?
- › Quel lien y a-t-il entre la stratégie en matière de risques et la stratégie opérationnelle ?
- › La politique de gestion des risques est-elle communiquée de manière claire au sein de la société ? Si oui, de quelle manière cela a-t-il été réalisé ? Dans le cas contraire, pourquoi ?
- › La politique en matière de prise de risques (les risques que l'entité est disposée à prendre) est-elle définie ? De quelle manière est-elle liée à ses objectifs ?
- › De quelle manière les positions du conseil<sup>1</sup> sur les risques ont-elles été diffusées dans la société ?

### Structure des risques

Approche visant à soutenir et incorporer la stratégie et les responsabilités en matière de risques.

- › Existe-t-il une terminologie et/ou un langage spécifique à la gestion des risques commun à l'ensemble de l'entité ? Dans le cas contraire, pourquoi ?
- › Au niveau de la direction, les responsabilités en matière de gestion des risques sont-elles clairement établies ? Si oui, de quelle manière cela a-t-il été réalisé ? Dans le cas contraire, pour quelles raisons ?
- › Les profils de poste font-ils état des responsabilités et/ou activités liées à la gestion des risques ?
- › Les systèmes de gestion de la performance et d'intéressement sont-ils cohérents avec les pratiques de l'entité en matière de gestion des risques ?

### Suivi et pilotage

Mise en place des indicateurs clés de performance (**Key Performance Indicators**), évaluation et amélioration en continu de la performance

- › Les propriétaires de risque sont-ils clairement identifiés ? Si oui, de quelle manière ? Dans le cas contraire, pourquoi ?
- › Des systèmes de mesure et de contrôle des risques ont-ils été mis en place ?
- › De quelle manière les risques, notamment les présomptions d'irrégularités, sont-ils transmis aux directions appropriées de l'entité ?
- › De quelle manière le système de gestion des risques est-il lié au système d'assurance de l'entité ?

## Système de gestion des risques

## Evaluation du système de gestion des risques

### Recensement des risques

Identification, évaluation et classement des risques au sein de l'entité.

- > Existe-t-il une cartographie des risques de l'entité ? Si ce n'est pas le cas, pour quelles raisons ?
- > La cartographie de risques met-elle en évidence l'identification et l'évaluation des expositions aux risques atypiques ?
- > Les corrélations entre les risques sont-elles clairement identifiées et comprises ?

### Risques opérationnels

- > Quels sont les risques opérationnels découlant de la stratégie ?
- > Comment l'entité identifie, évalue et gère-t-elle ces risques compte tenu de sa propension à accepter les risques ?
- > De quelle manière l'entité adapte-t-elle ses activités à l'évolution des stratégies et des processus ?

### Risques de réputation

- > Quels sont les risques pouvant affecter la marque et la réputation de l'entité ?

### Risques réglementaires ou contractuels

- > Quels sont les risques financiers et non financiers liés au respect des réglementations ou des accords contractuels ?

### Risques financiers

- > Les activités de l'entité exposent-elles les ressources financières à des risques excessifs ?
- > L'entité s'est-elle déraisonnablement endettée pour soutenir ses activités d'exploitation ?
- > L'entité a-t-elle réussi à satisfaire les objectifs mesurables opérationnels de la société ?

### Risques informatiques

- > Nos données, informations, connaissances sont-elles fiables et appropriées ?
- > Nos systèmes d'informations sont-ils fiables ?
- > Nos systèmes de sécurité sont-ils en ligne avec notre confiance dans la technologie, notamment concernant notre stratégie de e-business ?

### Nouveaux risques

- > Dans un environnement opérationnel en constante évolution, des processus d'identification des risques émergents ont-ils été mis en place ? Si oui, décrivez-les. Dans le cas contraire, pour quelles raisons ?
- > Quels risques pourraient encore apparaître ? Cela comprend les risques liés aux nouveaux concurrents ou aux nouveaux modèles d'activité, les risques de récession, les risques afférents aux relations avec des tiers, les risques liés à la sous-traitance, les risques politiques et pénaux, les risques financiers dus notamment à des partenaires commerciaux malhonnêtes, et autres risques de crises ou de catastrophes.

### Optimisation

Equilibre entre les risques potentiels et les opportunités en se fondant sur la propension à accepter les risques.

- > L'approche par les risques adoptée comprend-elle la recherche fréquente de nouveaux marchés, de nouvelles opportunités de partenariats et autres stratégies d'optimisation des risques ? Si oui, comment cela a-t-il été réalisé ? Dans le cas contraire, pour quelles raisons ?
- > Les risques sont-ils un facteur prédominant lors de la recherche de l'amélioration des processus de l'entreprise ? Si oui, décrivez comment cela est mis en place. Dans le cas contraire, pourquoi ?