Le management des risques de l’entreprise – Cadre de Référence

Synthèse

SYNTHESE

L'incertitude est une donnée intrinsèque à la vie de toute organisation. Aussi l'un des principaux défis pour la direction réside-t-il dans la détermination d'un degré d'incertitude acceptable afin d'optimiser la création de valeur, objectif considéré comme le postulat de base dans le concept de management des risques. L'incertitude est source de risques et d'opportunités, susceptibles de créer ou de détruire de la valeur. Le management des risques offre la possibilité d'apporter une réponse efficace aux risques et aux opportunités associés aux incertitudes auxquelles l'organisation fait face, renforçant ainsi la capacité de création de valeur de l'organisation.

La valeur de l'organisation est maximisée d'une part lorsque la direction élabore une stratégie et fixe des objectifs afin de parvenir à un équilibre optimal entre les objectifs de croissance et de rendement et les risques associés, et d'autre part lorsqu'elle déploie les ressources adaptées permettant d'atteindre ces objectifs. Le management des risques comprend les éléments suivants :

- *Aligner l'appétence pour le risque avec la stratégie de l'organisation* – L'appétence pour le risque est une donnée que la direction prend en considération lorsqu'elle évalue les différentes options stratégiques, détermine les objectifs associés et développe le dispositif pour gérer les risques correspondants.
- *Développer les modalités de traitement des risques* – Le dispositif de management des risques apporte une méthode permettant de choisir de façon rigoureuse parmi les différentes options de traitement des risques que sont : l'évitement, la réduction, le partage ou l'acceptation du risque.
- *Diminuer les déconvenues et les pertes opérationnelles* – Les organisations améliorent leur capacité à identifier et traiter les événements potentiels, ce qui leur permet d'atténuer les impondérables et de diminuer les coûts ou pertes associés.
- *Identifier et gérer les risques multiples et transverses* – Chaque entité est confrontée à une multitude de risques affectant différents niveaux de l'organisation. Le dispositif de management des risques renforce l'efficacité du traitement des impacts en cascade et apporte des solutions intégrées pour les risques à conséquences multiples.
- *Saisir les opportunités* – C'est en prenant en compte un large éventail d'événements potentiels que la direction est le mieux à même d'identifier et tirer parti des opportunités de façon proactive.
- *Améliorer l'utilisation du capital* – C'est en ayant une vision claire des risques de l'organisation que la direction peut évaluer efficacement les besoins en capitaux et en améliorer l'allocation.

Ces éléments du dispositif de management des risques, contribuent à la réalisation des objectifs de performance et de rentabilité de l'organisation et à la minimisation des pertes. Le dispositif de management des risques contribue aussi à la mise en place d'un reporting efficace et au respect de la conformité aux lois et réglementations. Ce faisant, il protège l'image de l'entité et lui épargne les conséquences néfastes d'une perte de réputation. En bref, grâce au déploiement d'un tel dispositif, une société est mieux armée pour atteindre ses objectifs et éviter les écueils et les impondérables.

Evénements – risques et opportunités

Les événements peuvent avoir un impact positif, négatif ou les deux à la fois. Les événements ayant un impact négatif sont des risques pouvant freiner la création de valeur ou détruire la valeur existante. En revanche, les événements ayant un impact positif peuvent contrebalancer des impacts négatifs des risques ou constituer des opportunités. Par opportunité, on entend la possibilité qu'un événement, en survenant, ait une incidence positive sur la réalisation d'objectifs et constitue un facteur de levier ou de soutien pour la création ou la préservation de valeur. La direction réintègre les opportunités identifiées dans le cadre du management des risques, à la réflexion stratégique et au processus de détermination des objectifs. Pour ce faire, il formule des plans permettant de saisir les opportunités.

Définition du management des risques

Le management des risques traite des risques et des opportunités ayant une incidence sur la création ou la préservation de la valeur. Il se définit comme suit :

> *Le management des risques est un processus mis en oeuvre par le conseil d'administration, la direction générale, le management et l'ensemble des collaborateurs de l'organisation.*
> *Il est pris en compte dans l'élaboration de la stratégie ainsi que dans toutes les activités de l'organisation. Il est conçu pour identifier les événements potentiels susceptibles d'affecter l'organisation et pour gérer les risques dans les limites de son appétence pour le risque. Il vise à fournir une assurance raisonnable quant à l'atteinte des objectifs de l'organisation.*

Cette définition reflète certains concepts fondamentaux. Le dispositif de management des risques :

- Est un processus permanent qui irrigue toute l'organisation
- Est mis en oeuvre par l'ensemble des collaborateurs, à tous les niveaux de l'organisation
- Est pris en compte dans l'élaboration de la stratégie
- Est mis en œuvre à chaque niveau et dans chaque unité de l'organisation et permet d'obtenir une vision globale de son exposition aux risques
- Est destiné à identifier les événements potentiels susceptibles d'affecter l'organisation, et à gérer les risques dans le cadre de l'appétence pour le risque
- Donne à la direction et au conseil d'administration une assurance raisonnable (quant à la réalisation des objectifs de l'organisation)
- Est orienté vers l'atteinte d'objectifs appartenant à une ou plusieurs catégories indépendantes mais susceptibles de se recouper

Cette définition est volontairement large. Elle intègre les principaux concepts sur lesquels s'appuient les sociétés ou d'autres types d'organisation pour définir leur dispositif de management des risques et se veut une base pour la mise en œuvre d'un tel dispositif au sein d'une organisation, d'un secteur industriel ou d'un secteur d'activité. Elle est centrée sur l'atteinte des objectifs fixés pour une entreprise donnée, et constitue en cela une base pour la définition d'un dispositif de management des risques efficace.

Atteinte des objectifs

Dans le cadre de la mission de l'organisation ainsi que de sa vision, la direction détermine des objectifs stratégiques, conçoit une stratégie et décline les objectifs qui en découlent à tous les niveaux de l'entité. Ce cadre de référence vise à aider l'organisation à atteindre ces objectifs que l'on peut classer dans les quatre catégories suivantes :

- *Stratégique* – objectifs stratégiques servant la mission de l'organisation
- *Opérationnel* – objectifs visant l'utilisation efficace et efficiente des ressources
- *Reporting* – objectifs liés à la fiabilité du reporting
- *Conformité* – objectifs de conformité aux lois et aux réglementations en vigueur

Ce rattachement des objectifs à différentes catégories permet de se concentrer sur différents aspects du management des risques. Tout en étant distinctes, ces catégories se recoupent - un objectif donné peut relever de plusieurs d'entre elles - et répondent aux divers besoins de l'entreprise. Elles peuvent relever de la responsabilité directe de différents dirigeants. Ce classement permet également de définir de façon plus précise les apports possibles pour chaque catégorie d'objectifs auxquelles certaines entités ajoutent la protection des actifs, également abordée dans cet ouvrage.

L'organisation ayant le contrôle sur les objectifs relatifs à la fiabilité du reporting et à la conformité aux lois et aux règlements, il est légitime d'attendre du processus de management des risques une assurance raisonnable quant à l'atteinte de ces objectifs. En revanche, l'atteinte des objectifs stratégiques et opérationnels dépend parfois d'événements extérieurs qui peuvent échapper au contrôle de l'entreprise. Par conséquent, dans ce cas, le management des risques ne peut donner qu'une assurance raisonnable que la direction et le conseil d'administration, dans son rôle de supervision, sont informés en temps utile de l'état de progression de l'organisation vers l'atteinte de ses objectifs.

Éléments du dispositif de management des risques

Le dispositif de management des risques comprend huit éléments. Ces éléments résultent de la façon dont l'organisation est gérée et sont intégrés au processus de management. Ces éléments sont les suivants :

- *Environnement interne* – L'environnement interne englobe la culture et l'esprit de l'organisation. Il structure la façon dont les risques sont appréhendés et pris en compte par l'ensemble des collaborateurs de l'entité, et plus particulièrement la conception du management et son appétence pour le risque, l'intégrité et les valeurs éthiques, et l'environnement dans lequel l'organisation opère.
- *Fixation des objectifs* – Les objectifs doivent avoir été préalablement définis pour que le management puisse identifier les événements potentiels susceptibles d'en affecter la réalisation. Le management des risques permet de s'assurer que la direction a mis en place un processus de fixation des objectifs et que ces objectifs sont en ligne avec la mission de l'entité ainsi qu'avec son appétence pour le risque.
- *Identification des événements* – Les événements internes et externes susceptibles d'affecter l'atteinte des objectifs d'une organisation doivent être identifiés en faisant la distinction entre risques et opportunités. Les opportunités sont prises en compte lors de l'élaboration de la stratégie ou au cours du processus de fixation des objectifs.
- *Evaluation des risques* – Les risques sont analysés, tant en fonction de leur probabilité que de leur impact, cette analyse servant de base pour déterminer la façon dont ils doivent être gérés. Les risques inhérents et les risques résiduels sont évalués.
- *Traitement des risques* – Le management définit des solutions permettant de faire face aux risques – évitement, acceptation, réduction ou partage. Pour ce faire le management élabore un ensemble de mesures permettant de mettre en adéquation le niveau des risques avec le seuil de tolérance et l'appétence pour le risque de l'organisation.

- *Activités de contrôle* – Des politiques et procédures sont définies et déployées afin de veiller à la mise en place et l'application effective des mesures de traitement des risques.
- *Information et communication* – Les informations utiles sont identifiées, collectées, et communiquées sous un format et dans des délais permettant aux collaborateurs d'exercer leurs responsabilités. Plus globalement, la communication doit circuler verticalement et transversalement au sein de l'organisation de façon efficace.
- *Pilotage* – Le processus de management des risques est piloté dans sa globalité et modifié en fonction des besoins. Le pilotage s'effectue au travers des activités permanentes de management ou par le biais d'évaluations indépendantes ou encore par une combinaison de ces deux modalités.

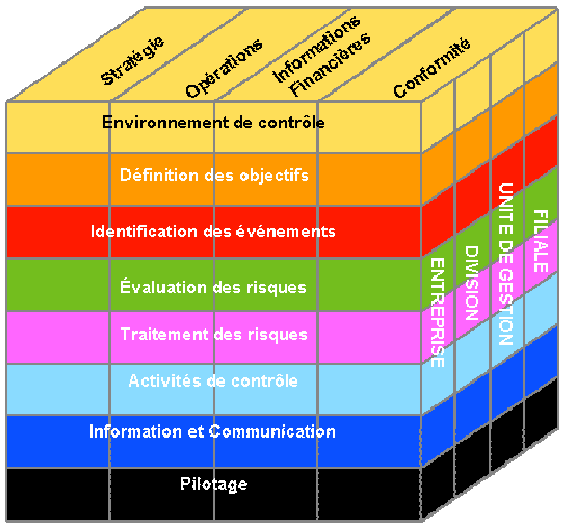
Le management des risques n'est pas un processus séquentiel dans lequel un élément affecte uniquement le suivant. C'est un processus multidirectionnel et itératif par lequel n'importe quel élément a une influence immédiate et directe sur les autres.

Relation entre objectifs et éléments

Il existe une relation directe entre les objectifs que cherche à atteindre une organisation et les éléments du dispositif de management des risques qui représentent ce qui est nécessaire à leur réalisation. La relation est illustrée par une matrice en trois dimensions ayant la forme d'un cube.

- Les quatre grandes catégories d'objectifs – stratégiques, opérationnels, reporting et conformité – sont représentées par les colonnes,
- les huit éléments du management des risques par les lignes
- et les unités de l'organisation par la troisième dimension.

Cette représentation illustre la façon d'appréhender le management des risques dans sa globalité ou bien par catégorie d'objectifs, par élément, par unité ou en les combinant.



Efficacité

L'efficacité d'un dispositif de management des risques peut s'apprécier en vérifiant que chacun des huit éléments est en place dans l'organisation et qu'ils fonctionnent efficacement. Ces éléments constituent donc un critère d'efficacité du dispositif de management des risques. Un dispositif efficace exclut toute faiblesse majeure dans l'un des éléments, et peut justifier que le niveau des risques est contenu dans les limites de l'appétence pour le risque de l'organisation.

Lorsque le dispositif de management des risques s'avère être efficacement géré pour chacune des quatre catégories d'objectifs, le conseil d'administration et la direction de l'organisation peuvent considérer qu'ils ont une assurance raisonnable de disposer d'une vision claire sur la façon dont les objectifs stratégiques et opérationnels de l'entreprise sont en passe d'être atteints, de la fiabilité du reporting et du respect des lois et règlements applicables.

La mise en œuvre et le fonctionnement des huit éléments est spécifique à chaque organisation. Pour les PME, le dispositif de management des risques peut être moins formel et moins structuré. Il n'en demeure pas moins que chacun des éléments existe et fonctionne correctement.

Limites

Si le dispositif de management des risques offre des avantages importants, il comporte néanmoins certaines limites. Outre les facteurs exposés ci-dessus, ces limites résultent :

- d'une erreur de jugement dans la prise de décision
- de la nécessaire prise en compte du rapport coûts / bénéfices dans le choix du traitement des risques, et de la mise en place des contrôles,
- de faiblesses potentielles dans le dispositif, susceptibles de survenir en raison de défaillances humaines (erreurs),
- de contrôles susceptibles d'être déjoués par collusion entre deux ou plusieurs individus,
- de la possibilité qu'a le management de passer outre les décisions prises en matière de gestion des risques.

En raison de ces limites un conseil d'administration ou une direction ne peuvent obtenir la certitude absolue que les objectifs de l'organisation seront atteints.

Intégration du contrôle interne

Le contrôle interne fait partie intégrante du dispositif de management des risques. Ce cadre de référence intègre le contrôle interne, constituant ainsi une modélisation et un outil de management plus « solide ». Le contrôle interne est défini et décrit dans l'ouvrage intitulé Internal Control – *Integrated Framework*[1]. Ce référentiel a fait ses preuves et constitue le fondement de règles, réglementations ou lois actuellement en vigueur et reste applicable comme référentiel du contrôle interne. Bien que seuls quelques extraits de Internal Control –*Integrated Framework* soient reproduits dans le présent document, l'intégralité du référentiel de contrôle interne est incorporé à cet ouvrage par le biais des références qui y sont faites.

Rôles et responsabilités

Le management des risques est l'affaire de tous mais, in fine, le directeur général en est le propriétaire et en assume la responsabilité. Les autres managers soutiennent la culture en matière de management des risques, ils oeuvrent pour sa mise en conformité avec l'appétence pour le risque et gèrent les risques au sein de leur périmètre de responsabilité dans les limites de la tolérance au risque. Le « risk manager », le directeur financier, l'auditeur interne et d'autres intervenants, assument habituellement des responsabilités fondamentales de support en matière de management des risques. Les autres collaborateurs de l'organisation sont responsables du dispositif de management des risques conformément aux directives et aux protocoles existants. Le conseil d'administration exerce une activité de surveillance sur le dispositif de management des risques, il a connaissance et valide l'appétence pour le risque de l'organisation. Certains tiers, tels que les clients, les fournisseurs, les partenaires commerciaux, les auditeurs externes, les régulateurs et les analystes financiers fournissent fréquemment des informations utiles au dispositif de management des risques, mais ils ne sont pas responsables de son efficacité et ne participent pas à sa mise en œuvre.

Structure de ce rapport

Ce rapport comporte deux parties. La première constitue le Cadre de référence proprement dit. Elle comprend aussi cette *Synthèse*. Le Cadre de référence définit le dispositif de management des risques, en décrit les principes et les concepts, et donne des principes directeurs pouvant être utilisés pour évaluer et renforcer l'efficacité du dispositif à tous les niveaux de l'organisation. La présente *Synthèse*

[1] Ouvrage traduit en français, par PricewaterhouseCoopers et l'IFACI sous le titre « La pratique du contrôle interne, COSO report ». Copyright en français IFACI.

est une vue d'ensemble destinée aux directions générales, aux collaborateurs occupant des postes clés, aux membres du conseil d'administration et aux régulateurs. La seconde partie, *Techniques d'application*, présente des exemples de techniques qui peuvent être utilisées pour la mise en œuvre des différents éléments du Cadre de référence.

Utilisation de ce rapport

Les actions possibles en lien avec ce rapport dépendent de la fonction et du rôle des parties impliquées :

- *Conseil d'administration* – Le conseil d'administration doit communiquer avec la direction générale sur le dispositif de management des risques en place dans l'organisation et exercer, si besoin est, un rôle de surveillance. Il doit s'assurer qu'il est informé des risques majeurs de l'organisation et des mesures prises par la direction pour les traiter, ainsi que de la façon dont elle s'assure de l'efficacité du dispositif. Pour ce faire, le conseil d'administration peut solliciter l'avis des auditeurs internes, des auditeurs externes et d'autres tiers.
- *Direction générale* – Dans cette étude, il est proposé que la direction générale évalue le dispositif de management des risques de l'organisation. En première approche, le directeur général peut par exemple réunir les responsables d'unités et les principaux responsables fonctionnels pour apprécier l'efficacité des éléments du dispositif en place. Quelle que soit sa forme, cette première approche doit déterminer la nécessité d'une évaluation plus approfondie et la façon dont elle doit être mise en œuvre.
- *Autres collaborateurs de l'organisation* – Les managers ainsi que les autres collaborateurs de l'organisation doivent analyser la manière dont ils exercent leurs responsabilités à la lumière de ce cadre de référence, et partager avec des collaborateurs plus expérimentés des suggestions pour renforcer le dispositif de management des risques. Les auditeurs internes doivent également réfléchir à l'étendue de leurs travaux dans le cadre du dispositif de management des risques.
- *Régulateurs* – Ce cadre de référence favorise le partage d'une vision commune du management des risques, notamment quant à son potentiel et ses limites. Ce modèle est donc susceptible de constituer une référence pour les régulateurs dans le cadre de la définition de leurs attentes en vue d'édicter des règles ou des directives ou lorsqu'ils procèdent à des contrôles.
- *Organismes professionnels* – Les organismes chargés d'établir des règles et les autres organismes professionnels établissant des directives en matière de gestion financière, d'audit ou de tout autre domaine apparenté devraient envisager les normes et recommandations qu'ils préconisent à la lumière de ce cadre de référence. Des concepts et une terminologie communs sont en effet bénéfiques à toutes les parties impliquées dans ce type de travaux.
- *Formateurs* – Ce cadre de référence peut faire l'objet de recherches et d'analyses universitaires permettant d'apporter des améliorations futures. Dans l'hypothèse où ce rapport deviendra un ouvrage de référence, ses concepts et sa terminologie devraient trouver leur place au sein des universités.

Forts d'une compréhension commune et partagée de la notion de management des risques, tous les acteurs seront à même de parler un langage commun et communiqueront de façon plus efficace. Les dirigeants d'organisations seront à même d'évaluer leur processus de management des risques comparativement à une norme, de le renforcer et d'aider leur entités à atteindre les objectifs fixés. Les recherches futures pourront capitaliser sur des bases existantes. Les législateurs et les régulateurs seront à même de mieux comprendre les processus de gestion des risques, notamment ses avantages et ses limites. Ces avantages se concrétiseront lorsque tous les acteurs utiliseront un référentiel commun de management des risques.