



Committee of Sponsoring Organizations of the Treadway Commission

Le management des risques de l'entreprise

Une démarche intégrée à la stratégie et à la performance

Synthèse



Traduit de l'anglais

Juin 2017

Ce projet a été commandité par le COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) qui, par un leadership éclairé, a vocation à élaborer des référentiels et des lignes directrices de premier plan concernant le contrôle interne, le management des risques de l'entreprise et la lutte contre la fraude, destinés à améliorer les performances et la surveillance de l'organisation et à réduire l'étendue de la fraude dans les organisations.

Le COSO est une initiative privée, pilotée et financée conjointement par :

- American Accounting Association
- American Institute of Certified Public Accountants
- Financial Executives International
- Institute of Management Accountants
- The Institute of Internal Auditors

Copyright © 2017 by Committee of Sponsoring Organizations of the Treadway Commission, ("COSO") strictly reserved. No parts of this material may be reproduced in any form without the written permission of COSO.

Permission has been obtained from the copyright holder, Committee of Sponsoring Organizations of the Treadway Commission to publish this translation, which is the same in all material respects, as the original unless approved as changed. No parts of this document may be reproduced, stored in any retrieval system, or transmitted in any form, or by any means electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of COSO.

©IFACI 2017, dans le seul cadre de ce document.

ISBN 978-2-915042-82-5

Avant-propos

Conformément à sa mission, le conseil du COSO avait commandité et publié en 2004 « *Le management des risques de l'entreprise — Cadre de référence* ». Au cours de la dernière décennie, les organisations ont largement adopté cette publication dans leurs démarches de gestion des risques. Cependant, cette période a également été marquée par l'évolution de la complexité des risques, l'émergence de nouveaux risques ainsi que la demande d'un reporting de plus en plus développé de la part des conseils et des dirigeants. Ce faisant, ces derniers ont amélioré leur connaissance et leur surveillance du management des risques de l'entreprise. Cette mise à jour de la publication de 2004 répond donc à l'évolution du management des risques de l'entreprise et au besoin pour les organisations d'améliorer leur approche de la gestion des risques pour répondre aux exigences d'un environnement économique mouvant.

Le document mis à jour, intitulé « *Le management des risques de l'entreprise — Une démarche intégrée à la stratégie et à la performance* », souligne l'importance de prendre en considération les risques tant dans le processus d'élaboration de la stratégie que dans le pilotage de la performance. Cette première partie de la mise à jour offre un aperçu des concepts et pratiques contemporains et émergents du management des risques de l'entreprise. La seconde partie, le *cadre de référence*, s'organise en cinq composantes, faciles à comprendre, qui s'adaptent à différentes structures organisationnelles, et améliorent la stratégie ainsi que la prise de décision. En résumé, cette mise à jour :

- éclaire l'intérêt du management des risques de l'entreprise lors de l'élaboration et de la mise en œuvre d'une stratégie ;
- renforce l'articulation entre la performance et le management des risques de l'entreprise afin d'améliorer la définition des objectifs de performance et la compréhension de l'impact des risques sur la performance ;
- tient compte des attentes en matière de gouvernance et de surveillance ;
- reconnaît la mondialisation des marchés et des activités ainsi que la nécessité d'avoir une approche à la fois commune et modulée selon les zones géographiques ;
- présente de nouvelles manières d'appréhender les risques liés à la définition et à la réalisation des objectifs dans un contexte de complexité accrue ;
- élargit le reporting pour répondre aux attentes d'une plus grande transparence de la part des parties prenantes ;
- tient compte de l'évolution des technologies et du foisonnement des données et des analyses requises pour étayer la prise de décisions ;
- propose des définitions, des composantes et des principes pour chaque niveau du management impliqué dans la conception, la mise en œuvre et le pilotage des pratiques de management des risques de l'entreprise.

Les lecteurs pourront également consulter une publication complémentaire du COSO, le « *Référentiel intégré de contrôle interne* ». Les deux publications sont distinctes et ont des objectifs différents ; aucune ne se substitue à l'autre mais elles sont reliées. Le « *Référentiel intégré de contrôle interne* » se focalise sur le contrôle interne, qui est en partie visé dans cette publication. Par conséquent, le référentiel intégré reste valable et approprié pour la conception, la mise en œuvre, le pilotage et l'évaluation du contrôle interne ainsi que pour le reporting y afférent.

Le conseil du COSO remercie PwC pour sa contribution significative à l'élaboration de cette publication : « *Le management des risques de l'entreprise — Une démarche intégrée à la stratégie et à la performance* ». Sa prise en compte des points de vue des nombreuses parties prenantes et son éclairage ont grandement contribué à assurer que les points forts de la publication originale soient conservés, et que le texte soit clarifié ou approfondi là où il était jugé utile de le faire. Le conseil du COSO et PwC remercient le comité consultatif et les observateurs pour leurs contributions à cette révision et pour leurs commentaires.



Robert B. Hirth Jr.
Président du COSO



Dennis L. Chesley
Partenaire PwC, chef du projet et responsable mondial pour la région Asie, Pacifique, Amériques de l'offre de services liés aux risques et à la conformité

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Administrateurs

Robert B. Hirth Jr.
Président du COSO

Richard F. Chambers
The Institute of Internal Auditors

Mitchell A. Danaher
Financial Executives International

Charles E. Landes
American Institute of Certified Public Accountants

Douglas F. Prawitt
American Accounting Association

Sandra Richtermeyer
Institute of Management Accountants

PwC—Auteur

Principaux contributeurs

Miles E.A. Everson
*Engagement Leader and Global and Asia, Pacific, and Americas (APA) Advisory Leader
New York, États-Unis*

Dennis L. Chesley
*Project Lead Partner and Global and APA Risk and Regulatory Leader
Washington DC, États-Unis*

Frank J. Martens
*Project Lead Director and Global Risk Framework and Methodology Leader
Colombie britannique, Canada*

Matthew Bagin
*Director
Washington DC, États-Unis*

Hélène Katz
*Director
New York, États-Unis*

Katie T. Sylvis
*Director
Washington DC, États-Unis*

Sallie Jo Perraglia
*Manager
New York, États-Unis*

Kathleen Crader Zelnik
*Manager
Washington, États-Unis*

Maria Grimshaw
*Senior Associate
New York, États-Unis*

Un éventail de risques évolutifs

Notre compréhension des risques, autrement dit l'art et la science de faire des choix, est au centre de l'économie moderne. Chaque choix que nous faisons pour atteindre des objectifs comporte des risques. Qu'il s'agisse de décisions courantes de gestion opérationnelle ou d'arbitrages cruciaux au niveau du conseil, traiter des risques associés à ces choix fait partie de la prise de décision.

Dans la recherche de l'optimisation d'une palette de résultats potentiels, les décisions sont rarement binaires, avec une bonne ou une mauvaise réponse. C'est pourquoi, le management des risques de l'entreprise peut à la fois être défini comme un art et une science. Ainsi, lorsque les risques sont pris en compte dans l'élaboration de la stratégie et des objectifs opérationnels d'une organisation, le management des risques de l'entreprise permet d'optimiser les résultats.

Notre compréhension des risques et notre pratique du management des risques de l'entreprise se sont considérablement améliorées pendant les dernières décennies. Dans le même temps, la marge d'erreur se réduit. Le Forum économique mondial a commenté « la volatilité, la complexité et l'ambiguïté croissantes du monde ».¹ C'est un phénomène connu de tous. Les organisations font face à des défis qui ont un impact sur leur robustesse, leur pertinence et la confiance qui leur est accordée. Les parties prenantes sont plus que jamais engagées et recherchent une transparence accrue dans la gestion de l'impact des risques et le devoir de rendre compte de cette gestion. Concomitamment, elles évaluent avec un regard critique la capacité du management à concrétiser des opportunités. Pourtant, même les succès ne sont pas sans risque de revers de fortune. Par exemple, le risque d'être dans l'incapacité de satisfaire à un accroissement imprévu de la demande ou de maintenir le niveau d'activité prévu.

Les organisations devront être à même de mieux s'adapter aux changements. Elles doivent se préparer stratégiquement à gérer la volatilité, la complexité et l'ambiguïté croissantes du monde. Ces réflexions doivent particulièrement avoir lieu au niveau de la direction et du conseil où les enjeux sont les plus importants.

Le management des risques de l'entreprise — Une démarche intégrée à la stratégie et à la performance donne un cadre de référence pour les conseils et le management des entités de toutes tailles. Il se fonde sur le niveau communément admis pour le management des risques dans les activités courantes. En outre, il démontre comment l'intégration des pratiques de management des risques à l'échelle de l'entreprise contribue à accélérer la croissance et à améliorer la performance. Il propose également des principes applicables de la prise de décision stratégique au pilotage de la performance.

Ci-après, nous indiquons pourquoi le management et les conseils² ont intérêt à utiliser le cadre de référence du management des risques de l'entreprise, les bénéfices déjà acquis par les organisations qui l'utilisent et les avantages supplémentaires qu'elles pourraient tirer de son utilisation permanente. Enfin, la conclusion porte un regard prospectif sur l'avenir.

Guide du management des risques à l'intention du management

La direction a la responsabilité globale de la gestion des risques à l'échelle de l'entité, mais il est important d'aller plus loin : renforcer le dialogue avec le conseil et les parties prenantes sur l'utilisation du management des risques de l'entreprise pour un avantage compétitif. Il convient alors de commencer par déployer des capacités de management des risques au cœur de la sélection d'une stratégie et de son élaboration.

Grâce à cette démarche, le management est mieux à même de comprendre comment la prise en compte explicite des risques peut avoir un impact sur le choix de la stratégie. Le management des risques de l'entreprise enrichit le dialogue en mettant en perspective les forces et faiblesses d'une stratégie lorsque les conditions changent, et la manière dont une stratégie s'inscrit dans la mission et la vision de l'organisation. Cela permet à la direction d'avoir l'assurance que les stratégies alternatives ont été examinées et que les points de vue de ceux qui, dans l'organisation, mettront en œuvre la stratégie sélectionnée ont été pris en compte.

¹ The Global Risks Report 2016, 11th edition, Forum économique mondial (2016).

² Les termes « conseil d'administration » ou « conseil » employés dans le *Cadre de référence* désignent l'organe de gouvernance, notamment les administrateurs, le conseil de surveillance, les fiduciaires, les associés commandités ou les actionnaires.

Une fois la stratégie définie, le management des risques de l'entreprise permet à la direction de remplir efficacement son rôle en sachant que les risques qui peuvent avoir un impact sur la stratégie de l'organisation sont connus et maîtrisés. Il contribue également à inspirer confiance aux parties prenantes et à leur donner une assurance dans le contexte actuel où une évaluation minutieuse de la manière dont le management envisage et gère ces risques est plus que jamais demandée.

Guide du management des risques à l'intention du conseil

Chaque conseil a un rôle de surveillance contribuant à soutenir la création de valeur dans une entité et à éviter son déclin. Jusqu'à présent, le management des risques de l'entreprise a fortement contribué aux activités du conseil. Désormais, cette instance est de plus en plus censée assurer la surveillance du management des risques de l'entreprise.

Le *Cadre de référence* propose aux conseils les principaux axes pour la définition et la réalisation de leurs responsabilités en matière de surveillance des risques. Les éléments à prendre en compte sont notamment : la gouvernance et la culture ; la stratégie et la définition des objectifs ; la performance ; l'information, la communication et le reporting, ainsi que la revue et l'amendement des pratiques pour accroître la performance de l'entité.

Sans être exhaustif, le rôle du conseil dans la surveillance des risques consiste notamment à :

- Réexaminer, discuter avec la direction, et s'accorder sur :
 - la stratégie proposée et l'appétence pour le risque ;
 - l'articulation de la stratégie et des objectifs opérationnels avec la mission, la vision et les valeurs fondamentales de l'entité ;
 - les décisions significatives pour l'organisation y compris les questions de fusion acquisition, d'allocation de capital, de financement et de dividende ;
 - la gestion des fluctuations significatives de performance de l'entité ou de portefeuille de risques ;
 - les réactions aux éventuels écarts par rapport aux valeurs fondamentales de l'organisation.

Questions à l'attention de la direction

Est-ce que chacun, au niveau du management — pas uniquement le directeur de la gestion des risques — peut expliciter la manière dont les risques sont envisagés dans la sélection de la stratégie ou dans les décisions opérationnelles ? Chacun peut-il énoncer clairement l'appétence pour le risque de l'entité et la manière dont elle pourrait influencer une décision spécifique ? Les réponses à ces questions peuvent donner un aperçu de l'état d'esprit concernant la prise de risques dans l'organisation.

Le conseil peut non seulement interroger la direction générale à propos des processus relatifs aux risques, mais également au sujet de la culture. Comment la culture permet-elle ou inhibe-t-elle la prise de risque responsable ? Quel point de vue le management adopte-t-il pour surveiller la culture du risque, et comment évolue-t-elle ? Au fil des évolutions — et les choses changent, que ce soit détecté ou non par l'entité —, comment le conseil peut-il avoir l'assurance que le management répondra de manière adéquate et en temps utile ?

- Approuver les mécanismes d'incitation et la rémunération des dirigeants.
- Participer aux échanges avec les investisseurs et les parties prenantes.

Sur le long terme, le management des risques de l'entreprise peut également accroître la résilience de l'organisation — sa capacité à anticiper les changements et à y répondre. Il aide les organisations à identifier les facteurs qui représentent non seulement un risque, mais également une mutation, et la manière dont ce changement pourrait affecter la performance et nécessiter une transformation de la stratégie. En identifiant plus clairement les mutations, une organisation peut modeler son plan stratégique : par exemple, faut-il rester sur la défensive ou investir dans une nouvelle activité ? Le management des risques de l'entreprise offre le cadre de référence adéquat pour que les conseils évaluent les risques et adoptent un état d'esprit de résilience.

Les acquis du management des risques de l'entreprise

Le COSO a publié *Le management des risques de l'entreprise — cadre de référence* en 2004. L'objectif était d'aider les entités à mieux protéger et accroître la valeur pour leurs parties prenantes. La philosophie sous-jacente était que « la valeur est maximisée lorsque la direction fixe une stratégie et des objectifs permettant d'optimiser l'équilibre entre croissance, rentabilité et risques associés, ou encore lorsqu'un déploiement efficace et efficient des ressources permet d'atteindre les objectifs de l'organisation ». ³

³ *Le management des risques de l'entreprise - cadre de référence*, synthèse, COSO (2004).

Depuis sa publication, ce *Cadre de référence* a été utilisé avec succès dans le monde entier, dans tous les secteurs, et dans des organisations de tous types et de toutes tailles, pour identifier les risques dans les limites d'une appétence pour le risque définie et contribuer ainsi à l'atteinte des objectifs. Pourtant, malgré le nombre important d'utilisateurs actuels, le potentiel du *Cadre de référence* n'est pas encore complètement exploité. Certains aspects pourraient en effet être approfondis et clarifiés en offrant une meilleure compréhension des liens entre la stratégie, les risques et la performance. Dans cet esprit, l'actualisation du *Cadre de référence* :

- relie plus explicitement le management des risques de l'entreprise à une multitude d'attentes des parties prenantes ;
- situe les risques dans le cadre de la performance de l'organisation, au lieu de les voir comme le sujet d'un exercice isolé ;
- permet aux organisations de mieux anticiper les risques afin de prendre les devants, en comprenant que le changement est source d'opportunités, pas seulement de crises potentielles.

Cette mise à jour répond également à l'invitation pressante d'une attention particulière sur la manière dont le management des risques éclaire la stratégie et la performance de l'organisation.

Les bénéfices d'un management des risques de l'entreprise efficace

Toutes les organisations ont besoin de définir une stratégie et de l'ajuster régulièrement, en ayant à la fois conscience des opportunités en perpétuelle évolution de création de valeur et des défis à relever pour la concrétisation de cette valeur. Elles ont donc besoin du meilleur cadre de référence possible pour optimiser la stratégie et la performance.

C'est là que le management des risques de l'entreprise entre en jeu. Les organisations qui intègrent le management des risques dans toute l'entité peuvent en tirer de nombreux bénéfices, y compris et sans vouloir être exhaustif :

- *Accroître la gamme des opportunités* : en tenant compte de toutes les éventualités — les aspects positifs ainsi que négatifs des risques — le management peut identifier de nouvelles opportunités et des enjeux spécifiques liés aux opportunités actuelles.
- *Identifier et gérer les risques à l'échelle de l'entité* : chaque entité est confrontée à une multitude de risques qui peuvent affecter de nombreux domaines de l'organisation. Quelquefois, un risque peut naître dans une partie d'une entité, mais avoir un impact sur une autre partie. Par conséquent, le management identifie et gère ces risques à l'échelle de l'entité pour maintenir et améliorer la performance.
- *Augmenter les résultats positifs et les bénéfices en réduisant les mauvaises surprises* : le management des risques de l'entreprise permet aux entités d'améliorer leur capacité à identifier les risques et à y apporter des réponses adéquates, en réduisant les surprises ainsi que les coûts ou les pertes qui en découlent, tout en profitant de développements intéressants.

Mise au point à propos de quelques fausses idées

Depuis sa publication en 2004, le *Cadre de référence* a suscité de fausses idées. Pour dissiper tout malentendu :

Le management des risques de l'entreprise n'est ni une fonction ni un département. C'est la culture, les capacités et les pratiques que les organisations intègrent à l'élaboration de la stratégie et appliquent lorsqu'elles mettent en œuvre cette stratégie, dans le but de gérer les risques en créant de la valeur, en la préservant et en la concrétisant.

Le management des risques de l'entreprise n'est pas une énumération des risques. Plus que l'inventaire de tous les risques d'une organisation, il s'agit des pratiques managériales mises en œuvre pour gérer activement les risques.

Le management des risques de l'entreprise va au-delà du contrôle interne. Il s'intéresse également à d'autres sujets comme l'élaboration de la stratégie, la gouvernance, la communication avec les parties prenantes et la mesure de la performance. Ses principes s'appliquent à tous les niveaux de l'organisation et dans chaque fonction.

Le management des risques de l'entreprise n'est pas une liste de points de contrôle. C'est un ensemble de principes pour définir ou intégrer les processus d'une organisation donnée. C'est un système de pilotage, d'apprentissage et d'amélioration de la performance.

Le management des risques de l'entreprise peut être utilisé par des organisations de toutes tailles. A partir du moment où une organisation a une mission, une stratégie et des objectifs — et la nécessité de prendre des décisions qui tiennent pleinement compte des risques — alors le management des risques de l'entreprise est applicable. Il peut et devrait être utilisé par tous types d'organisations, des petites entreprises à celles qui investissent dans l'économie sociale et solidaire ; des établissements publics aux grandes capitalisations boursières.

- *Réduire la volatilité de la performance* : pour certains, l'enjeu réside moins dans les surprises et les pertes que dans la volatilité de la performance. Etre en avance par rapport aux échéances initiales ou dépasser les prévisions peut causer autant de problèmes qu'être en retard ou être en-deçà des prévisions. Le management des risques de l'entreprise permet aux organisations d'anticiper les risques qui affecteraient la performance et leur donne les moyens de mettre en place les actions nécessaires pour minimiser les perturbations et maximiser les opportunités.
- *Améliorer le déploiement des ressources* : on peut considérer qu'à chaque risque correspond un besoin en ressources. Dans un contexte de ressources limitées, l'obtention d'informations solides sur les risques permet au management d'évaluer les besoins globaux en ressources, de fixer des priorités pour leur déploiement et d'améliorer leur allocation.
- *Accroître la résilience de l'organisation* : la viabilité à moyen et long terme d'une entité dépend de sa capacité à anticiper les évolutions et à y répondre, non seulement pour survivre, mais aussi pour évoluer et prospérer. Elle est, en partie, facilitée par un management des risques de l'entreprise efficace. Cet aspect devient de plus en plus important compte tenu de l'accélération du rythme des mutations et de la complexité croissante des organisations.

Ces bénéfices soulignent le fait que les risques ne devraient pas être perçus comme des contraintes ou des obstacles potentiels à l'élaboration et à la mise en œuvre d'une stratégie. Au contraire, les évolutions qui suscitent des risques et les réponses que l'organisation apporte à ces risques sont autant d'opportunités stratégiques et de facteurs clés de différenciation.

La place des risques dans la sélection de la stratégie

Sélectionner une stratégie, c'est faire des choix et accepter des arbitrages. Il est donc logique d'appliquer le management des risques de l'entreprise à la stratégie, car c'est le meilleur moyen de mettre en œuvre l'art et la science de faire des choix éclairés.

Les risques sont pris en compte dans de nombreux processus d'élaboration de la stratégie. Mais les risques sont souvent essentiellement évalués par rapport à leurs impacts potentiels sur une stratégie donnée. En d'autres mots, la discussion porte sur les risques relatifs à la stratégie existante : nous avons une stratégie en place, qu'est-ce qui pourrait affecter l'adéquation et la viabilité de cette stratégie ?

Mais il y a d'autres questions à se poser à propos de la stratégie : avons-nous correctement modélisé la demande des clients ? Notre chaîne d'approvisionnement livrera-t-elle dans les délais et en respectant le budget ? De nouveaux concurrents émergeront-ils ? Notre infrastructure technologique est-elle à la hauteur de la tâche ? Ce sont ce type de questions auxquelles les dirigeants sont quotidiennement confrontés, et il est fondamental d'y répondre pour mener à bien une stratégie.

Les risques relatifs à la stratégie sélectionnée ne sont qu'un des aspects à prendre en compte. Comme ce *Cadre de référence* le souligne, il existe deux aspects supplémentaires du management des risques de l'entreprise qui peuvent avoir un impact beaucoup plus important sur la valeur d'une entité : l'éventualité que la stratégie ne soit pas alignée, et les conséquences de la stratégie sélectionnée.

Tout d'abord, **l'éventualité que la stratégie ne soit pas alignée avec la mission, la vision et les valeurs fondamentales d'une organisation** est au cœur des décisions qui sous-tendent la sélection de la stratégie. Chaque entité a une mission, une vision, et des valeurs fondamentales qui définissent ce à quoi elle essaie de parvenir et la manière dont elle veut mener ses activités. Certaines organisations sont sceptiques quant à l'intérêt d'adopter entièrement ces principes. Cependant la mission, la vision et les valeurs fondamentales sont essentielles — et le sont d'autant plus quand il s'agit de gérer les risques et de rester résilient en périodes de mutation.

La stratégie sélectionnée doit soutenir la mission et la vision de l'organisation. Une stratégie en déphasage augmente la possibilité que l'organisation ne réalise ni sa mission ni sa vision, ou peut compromettre ses valeurs, même si la stratégie est exécutée avec succès. Par conséquent, le management des risques de l'entreprise prend en compte la possibilité que la stratégie ne soit pas alignée avec la mission et la vision d'une organisation.

Un autre aspect concerne les **conséquences de la stratégie sélectionnée**. Quand la direction élabore une stratégie et analyse les alternatives avec le conseil, elle prend des décisions sur les arbitrages inhérents à la stratégie. Chaque stratégie alternative a son propre profil de risque correspondant aux conséquences qui découlent de cette stratégie. Le conseil et la direction générale doivent déterminer si la stratégie est ajustée à l'appétence pour le risque de l'organisation, et comment elle orientera l'organisation dans la fixation des objectifs pour in fine allouer de manière efficiente ses ressources.

Il est important de comprendre que le management des risques de l'entreprise est tout autant une question de compréhension des conséquences de la stratégie et de l'éventualité que la stratégie ne soit pas alignée qu'une question de gestion des risques relatifs aux objectifs fixés. Le diagramme ci-dessous illustre une prise en considération de ces éléments dans le contexte de la mission, de la vision et des valeurs fondamentales, et en tant que levier pour le pilotage global et la performance d'une entité.



Le management des risques de l'entreprise, tel qu'il est habituellement pratiqué, a aidé de nombreuses organisations à identifier, évaluer et gérer les risques liés à la stratégie. Mais les causes les plus importantes de destruction de valeur résident dans la possibilité que la stratégie ne soutienne pas la mission et la vision de l'entité, et dans les conséquences de cette stratégie.

Le management des risques de l'entreprise améliore le choix d'une stratégie. Sélectionner une stratégie requiert une prise de décision méthodique en analysant les risques et en ajustant les ressources à la mission et à la vision de l'organisation.

Un cadre de référence ciblé






Le management des risques de l'entreprise — Une démarche intégrée à la stratégie et à la performance précise l'importance du management des risques dans la planification stratégique et dans l'intégration de la stratégie à travers l'organisation. En effet, dans tous les départements et dans toutes les fonctions, les risques influencent et ajustent la stratégie et la performance.



Le *Cadre de référence* propose un ensemble de principes organisés en cinq composantes interdépendantes :

- 1. Gouvernance et culture** : la gouvernance donne le ton dans l'organisation, en insistant sur l'importance du management des risques de l'entreprise et en définissant les responsabilités de surveillance de cette démarche. La culture correspond aux valeurs éthiques, aux comportements souhaités et à la compréhension des risques dans l'entité.
- 2. Stratégie et définition des objectifs** : le management des risques de l'entreprise, la stratégie et la définition des objectifs contribuent conjointement au processus de planification stratégique. L'appétence pour le risque est définie et ajustée à la stratégie ; les objectifs opérationnels permettent de mettre en œuvre la stratégie tout en servant de base pour l'identification, l'évaluation et le traitement des risques.
- 3. Performance** : les risques qui peuvent affecter la réalisation de la stratégie et des objectifs opérationnels doivent être identifiés et évalués. Les risques sont priorisés selon leur criticité dans le contexte de l'appétence pour le risque de l'organisation. L'organisation sélectionne ensuite les modalités de traitement des risques et analyse en termes de portefeuille le niveau de risque assumé. Les résultats de ce processus sont communiqués aux parties prenantes clés concernées par les risques.
- 4. Revue et amendement** : en examinant la performance de l'entité, une organisation peut prendre en considération la manière dont les composantes du management des risques fonctionnent au fil du temps, et en fonction de changements substantiels, ainsi que les éventuels amendements nécessaires.
- 5. Information, communication et reporting** : le management des risques de l'entreprise exige un processus permanent d'obtention et de partage des informations nécessaires, provenant de sources internes et externes, qui sont transmises de façon ascendante, descendante ou transversale dans l'organisation.

Les cinq composantes du *Cadre de référence* mis à jour s'appuient sur un ensemble de principes.⁴ Ces principes vont de la gouvernance au pilotage. D'un nombre raisonnable, ils définissent des pratiques applicables de différentes manières dans des organisations de taille, type ou secteur divers. En adoptant ces principes, la direction générale et le conseil peuvent raisonnablement attendre de l'organisation qu'elle comprenne et s'efforce de gérer les risques associés à sa stratégie et ses objectifs opérationnels.

 Gouvernance et culture	 Stratégie et définition des objectifs	 Performance	 Revue et amendement	 Information, communication, et reporting
<ol style="list-style-type: none"> 1. Exercer une surveillance des risques par le conseil 2. Définir les structures organisationnelles 3. Définir la culture souhaitée 4. Démontrer l'engagement en faveur de valeurs fondamentales 5. Attirer, former et fidéliser des personnes compétentes 	<ol style="list-style-type: none"> 6. Analyser le contexte de l'organisation 7. Définir l'appétence pour le risque 8. Évaluer les stratégies alternatives 9. Définir les objectifs opérationnels 	<ol style="list-style-type: none"> 10. Identifier les risques 11. Évaluer la criticité des risques 12. Prioriser les risques 13. Mettre en œuvre les modalités de traitement des risques 14. Développer une vision globale du portefeuille de risques 	<ol style="list-style-type: none"> 15. Évaluer les changements substantiels 16. Réexaminer les risques et la performance 17. Poursuivre l'amélioration du management des risques de l'entreprise 	<ol style="list-style-type: none"> 18. Tirer parti des données et des technologies 19. Communiquer les informations relatives aux risques 20. Rendre compte des risques, de la culture et de la performance

Quelques perspectives futures

Il n'y a aucun doute que, dans le futur, les organisations continueront à faire face à la volatilité, la complexité et l'ambiguïté. Le management des risques de l'entreprise jouera un rôle important dans la manière dont une organisation est gérée et prospère dans ce contexte. Indépendamment du type et de la taille d'une entité, sa stratégie doit rester fidèle à sa mission. De plus, chaque entité doit être en mesure d'explicitier des spécificités qui susciteront des réponses efficaces au changement, notamment par :

- des prises de décisions rapides et souples ,
- la capacité d'agir de manière cohérente ;
- la capacité d'adaptation qui aide à pivoter et à se repositionner ;
- le maintien d'un niveau de confiance élevé de la part des parties prenantes.

Dans le futur, différentes tendances auront un impact sur le management des risques de l'entreprise. A titre d'exemple, citons les quatre tendances suivantes :

- *La prise en compte du foisonnement des données* : alors que de plus en plus de données deviennent disponibles et que la vitesse à laquelle peuvent être analysées ces nouvelles données augmente, le management des risques de l'entreprise devra s'adapter. Les données viendront à la fois de l'intérieur et de l'extérieur de l'entité, et elles seront structurées de manières différentes. Des outils perfectionnés d'analyse et de visualisation des données évolueront et seront très utiles pour comprendre les risques et leurs impacts — à la fois positifs et négatifs.
- *L'utilisation de l'intelligence artificielle et l'automatisation* : de nombreuses personnes considèrent que nous sommes dans l'ère des processus automatisés et de l'intelligence artificielle. Indépendamment de ces points de vue, il est important que le management des risques de l'entreprise prenne en compte l'impact des technologies présentes et futures, et tire parti de leurs potentiels. Des liens, tendances et scénarios indétectables auparavant peuvent désormais l'être en offrant une source précieuse d'informations essentielles pour le management des risques.
- *La maîtrise du coût du management des risques* : une préoccupation fréquemment exprimée par les dirigeants concerne le coût du management des risques, des processus de conformité et des activités de contrôle comparé à leur valeur ajoutée. Comme les pratiques de management des risques de l'entreprise évoluent, il deviendra essentiel que les activités concernant les risques, la conformité, le contrôle et même la gouvernance soient coordonnées de manière efficace pour que l'organisation puisse en tirer le maximum de bénéfices. Ce serait l'une des meilleures façons de conforter l'importance du management des risques de l'entreprise pour chaque organisation.

⁴ Une description plus complète de ces vingt principes est fournie à la fin de ce document.

- *Le renforcement de la robustesse des organisations* : plus les organisations progressent dans l'intégration du management des risques de l'entreprise à la stratégie et à la performance, plus elles ont l'opportunité de renforcer leur résilience. En connaissant les risques qui auront le plus d'impact sur l'entité, les organisations peuvent utiliser le management des risques de l'entreprise pour les aider à mettre en place des capacités d'actions proactives. Autant de pistes pour de nouvelles opportunités.

En résumé, le management des risques de l'entreprise devra évoluer et s'adapter au futur pour offrir systématiquement les bénéfices soulignés dans le *Cadre de référence*. Avec une attention adéquate, les bénéfices qui découlent du management des risques de l'entreprise excéderont de loin les investissements et donneront confiance aux organisations dans leurs capacités à aborder l'avenir.

Remerciements

Le COSO remercie les sociétés et organisations suivantes qui ont permis la contribution de membres du comité consultatif et d'observateurs.

Membres du comité consultatif

Société et organisations

- Athene USA (Jane Karli)
- Edison International (David J. Heller)
- First Data Corporation (Lee Marks)
- Georgia-Pacific LLC (Paul Sobel)
- Invesco Ltd. (Suzanne Christensen)
- Microsoft (Jeff Pratt)
- US Department of Commerce (Karen Hardy)
- United Technologies Corporation (Margaret Boissoneau)
- Zurich Insurance Company (James Davenport)

Enseignement supérieur et associations

- North Carolina State University (Mark Beasley)
- St. John's University (Paul Walker)
- The Institute of Internal Auditors (Douglas J. Anderson)

Prestataires de services professionnels

- Crowe Horwath LLP (William Watts)
- Deloitte & Touche LLP (Henry Ristuccia)
- Ernst & Young (Anthony J. Carmello)
- James Lam & Associates (James Lam)
- Grant Thornton LLP (Bailey Jordan)
- KPMG LLP Americas (Deon Minnaar)
- Mercury Business Advisors Inc. (Patrick Stroh)
- Protiviti Inc. (James DeLoach)

Anciens administrateurs du COSO

- Président du COSO, 2009–2013 (David Landsittel)

Observateurs

- Federal Deposit Insurance Corporation (Harrison Greene)
- Government Accountability Office (James Dalkin)
- Institute of Management Accountants (Jeff Thompson)
- Institut der Wirtschaftsprüfer (Horst Kreisel)
- International Federation of Accountants (Vincent Tophoff)
- ISACA (Jennifer Bayuk)
- Risk Management Society (Carol Fox)

Réviseurs de la traduction effectuée par l'IFACI

L'IFACI remercie les professionnels qui ont contribué à la révision de la traduction en français :

- Bruno Buresi, AMF
- Christophe Butikofer, Unedic
- Jérôme Cantiant, Eramet
- Vianney Dumont, Maif
- Béatrice Ki-Zerbo, IFACI
- Sébastien Lepers, Cour des comptes
- Stephan Roudil, Comité d'harmonisation de l'audit interne, Ministère de l'économie

Leurs contributions, à titre individuel, n'engagent pas leur organisation.

Composantes et principes

- 1. Exercer une surveillance des risques par le conseil** — Le conseil assure la surveillance de la stratégie et assume les responsabilités en matière de gouvernance pour soutenir la direction générale dans la réalisation de la stratégie et des objectifs opérationnels.
- 2. Définir les structures organisationnelles** — L'organisation définit des structures organisationnelles dans la perspective de la réalisation de la stratégie et des objectifs opérationnels.
- 3. Définir la culture souhaitée** — L'organisation définit les comportements attendus qui caractérisent la culture souhaitée par l'entité.
- 4. Démontrer l'engagement en faveur de valeurs fondamentales** — L'organisation démontre son engagement pour les valeurs fondamentales de l'entité.
- 5. Attirer, former et fidéliser des personnes compétentes** — L'organisation s'engage à développer le capital humain en adéquation avec la stratégie et les objectifs opérationnels.
- 6. Analyser le contexte de l'organisation** — L'organisation prend en considération l'impact potentiel de son contexte sur le profil de risque.
- 7. Définir l'appétence pour le risque** — L'organisation définit l'appétence pour le risque dans le contexte de la création, de la préservation et de la concrétisation de la valeur.
- 8. Évaluer les stratégies alternatives** — L'organisation évalue les stratégies alternatives et leurs impacts potentiels sur le profil de risque.
- 9. Définir les objectifs opérationnels** — L'organisation prend en considération les risques lors de la définition, à différents niveaux, d'objectifs opérationnels qui soient en phase avec la stratégie et la soutiennent.
- 10. Identifier les risques** — L'organisation identifie les risques qui affectent la réalisation de la stratégie et des objectifs opérationnels.
- 11. Évaluer la criticité des risques** — L'organisation évalue la criticité des risques.
- 12. Prioriser les risques** — L'organisation priorise les risques pour sélectionner les modalités de traitement de ces risques.
- 13. Mettre en œuvre les modalités de traitement des risques** — L'organisation identifie et sélectionne les modalités de traitement des risques.
- 14. Développer une vision globale du portefeuille de risques** — L'organisation développe une vision globale et une évaluation du portefeuille de risques.
- 15. Évaluer les changements substantiels** — L'organisation identifie et évalue les changements qui pourraient affecter substantiellement la stratégie et les objectifs opérationnels.
- 16. Réexaminer les risques et la performance** — L'organisation revoit la performance de l'entité et prend en considération les risques.
- 17. Poursuivre l'amélioration du management des risques de l'entreprise** — L'organisation poursuit l'amélioration du management des risques de l'entreprise.
- 18. Tirer parti des données et des technologies** — L'organisation exploite les systèmes d'information et technologiques de l'entité pour soutenir le management des risques de l'entreprise.
- 19. Communiquer les informations relatives aux risques** — L'organisation utilise les moyens de communication pour soutenir le management des risques de l'entreprise.
- 20. Rendre compte des risques, de la culture et de la performance** — L'organisation rend compte des risques, de la culture et de la performance à différents niveaux et dans toute l'entité.



L'ouvrage « *Enterprise Risk Management - Integrating with strategy and performance* » est en vente sur le site internet www.coso.org.