Gestion du risque en entreprise

UNE APPROCHE PRATIQUE DE LA GESTION DES RISQUES POUR LES PETITES ET MOYENNES ORGANISATIONS

Bill Wesioly et Guenther Moeller

Quel est l'enjeu?
Les résultats d'un sondage mené en 2018[1] ont montré que près de la moitié des petites et moyennes organisations n'avaient aucun programme de gestion du risque en entreprise (GRE).

Or, ces organisations exercent leurs activités dans des environnements complexes et exigeants qui ne cessent d'évoluer. Pour éviter le plus possible les pertes d'exploitation inattendues et pour atteindre leurs objectifs, elles doivent continuellement prendre des décisions à la fois rapides et éclairées concernant les stratégies et les activités. D'où l'utilité d'adopter une approche globale et des pratiques judicieuses en matière de gestion des risques.

Pourquoi est-ce important?
Intégrées de façon stratégique, des pratiques concrètes de gestion des risques qui sont bien arrimées aux besoins opérationnels peuvent aider les organisations de petite et de moyenne taille, y compris les organismes sans but lucratif (OSBL), à atteindre leurs objectifs, à accroître la valeur pour les parties prenantes, et à respecter les exigences au chapitre de la gouvernance et de la conformité.

Que peut-on faire?
Dans les présentes lignes directrices, vous trouverez des indications qui vous aideront à composer avec les dynamiques internes et externes (et les risques associés) qui ont une incidence sur vos objectifs stratégiques et sur les activités quotidiennes de l'organisation. Vous découvrirez comment : mettre en œuvre des pratiques de gestion des risques explicites, structurées et intégrées; répondre aux besoins en matière de contrôle interne; et créer une culture du risque favorisant l'efficacité du processus décisionnel.

Bon nombre d'organisations mettent en place un programme de gestion des risques seulement après avoir connu une situation difficile (comme la perte d'un important client, une amende salée ou une poursuite importante). Grâce aux présentes lignes directrices, il vous sera plus facile de prévoir ce genre de situation et d'y réagir plus tôt, puis d'en gérer et d'en réduire au minimum les incidences.

À qui les lignes directrices s'adressent-elles?
Les présentes lignes directrices sont destinées aux personnes (souvent des CPA) chargées de l'établissement et de la réalisation des objectifs de l'organisation et, dans bien des cas, de la gestion des risques s'y rattachant. Autrement dit, l'auditoire cible comprend :

- les membres du conseil d'administration qui exercent une surveillance à l'égard de la gestion des risques;
- les hauts dirigeants qui sont responsables de l'élaboration de stratégies et de la prise de décisions (par exemple, le chef des finances, le chef de la direction, l'auditeur en chef);
- les cadres hiérarchiques et d'autres membres du personnel d'exploitation.

Dans les présentes lignes directrices, les petites et moyennes organisations s'entendent des organisations qui comptent moins de 100 employés. Les lignes directrices peuvent toutefois s'appliquer à certaines organisations de plus grande taille, dans différents secteurs et industries.

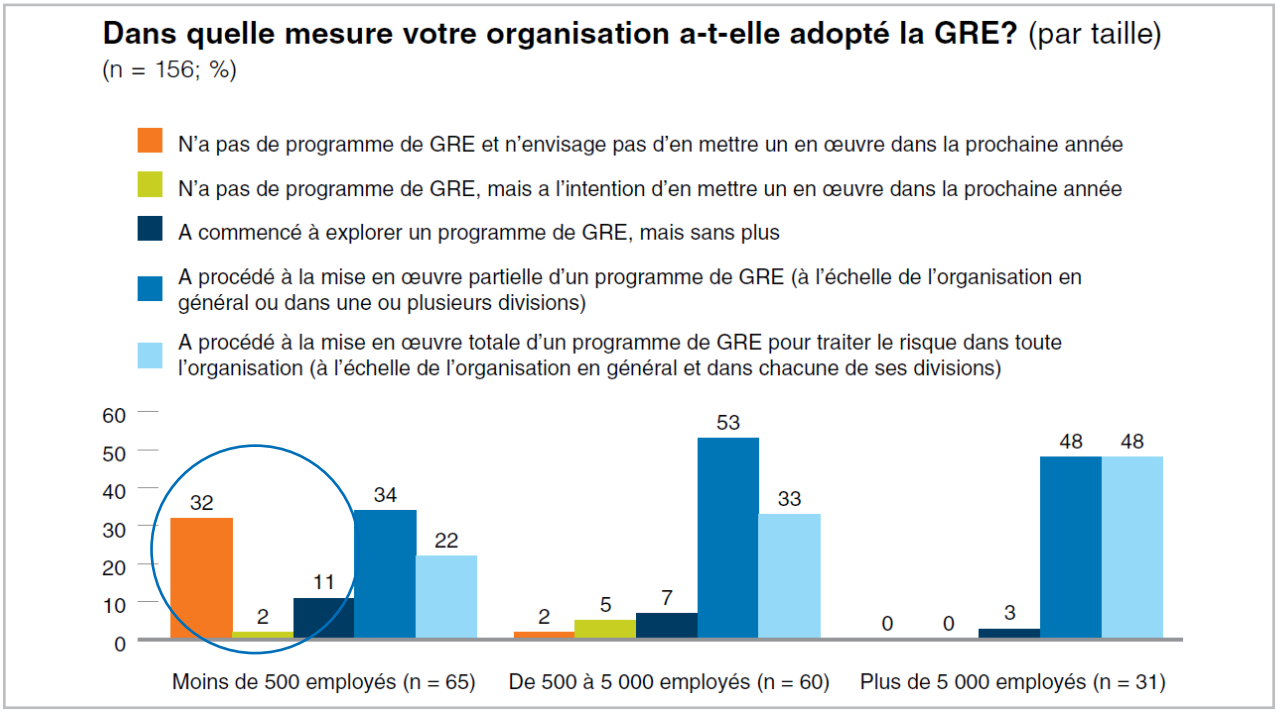
1 Le sondage ***L'état de la GRE au Canada : enquête d'étalonnage*** (2018) a été réalisé conjointement par le Conference Board du Canada, Comptables professionnels agréés du Canada (CPA Canada) et l'Institut mondial de gestion des risques du secteur financier.

Vue d'ensemble

Incidence des tendances qui se dessinent sur votre organisation

Selon un sondage canadien mené en 2018, près de 50 % des petites et moyennes organisations n'ont aucun programme de gestion du risque en entreprise (GRE)[2] – ce terme étant défini, dans le sondage, comme un programme qui fournit une approche structurée pour gérer globalement les risques opérationnels et stratégiques et qui établit un lien entre les risques et les objectifs stratégiques et opérationnels (figure 1).

FIGURE 1 – DANS QUELLE MESURE VOTRE ORGANISATION A-T-ELLE ADOPTÉ LA GRE?



Cette figure est frappante, particulièrement dans le contexte des récentes manchettes qui illustrent les répercussions considérables au chapitre de la réputation et sur le plan financier pour les organisations concernées. Voici quelques exemples :

- Escroquerie par hameçonnage : une municipalité s'est fait voler 503 000 $;
- Nouvelles accusations d'agressions dans une école privée après que la vidéo d'un cellulaire est devenue virale;

2 Le sondage *L'état de la GRE au Canada : enquête d'étalonnage* (2018) a été réalisé conjointement par le Conference Board du Canada, Comptables professionnels agréés du Canada (CPA Canada) et l'Institut mondial de gestion des risques du secteur financier.

- Réduction de 15 millions de dollars de la fondation du gouvernement provincial : une différence considérable pour les organismes sans but lucratif et les organismes de bienfaisance.

De nombreuses organisations tentent de mettre en place un programme de gestion des risques après qu'un événement négatif est survenu. Les présentes lignes directrices aideront les lecteurs à adopter une approche rigoureuse et globale aux fins de la gestion des nombreux risques actuels et nouveaux au sein de leur organisation.

La pandémie de 2019 a mis à l'épreuve la poursuite des activités. Elle a constitué un événement de risque majeur qui a exigé des organisations qu'elles prennent des mesures immédiates pour gérer les risques ayant une incidence sur leur personnel, leurs activités et leur viabilité financière. Ces mesures comprenaient la mise à l'essai des plans de continuité des activités, des systèmes de gestion des urgences et de la préparation aux catastrophes (se reporter à la section 6.2, « Analyse des hypothèses les plus défavorables »). En ces temps d'incertitude sans précédent, de changement constant et de perturbation des activités, la viabilité à long terme d'une organisation dépend de sa capacité :

- à faire preuve de résilience face à l'incertitude;
- à adapter ses pratiques commerciales aux pressions concurrentes du marché;
- à innover continuellement avec des idées originales afin de créer une valeur durable à long terme.

CPA Canada a élaboré son cadre RAID[3] pour aider les organisations à évaluer leur résilience, leur adaptabilité et leur capacité d'innover face au changement afin d'assurer leur continuité et leur viabilité. La mise en œuvre de saines stratégies et pratiques de gestion des risques vient appuyer ce cadre.

Prendre un risque peut également générer des rendements et de la valeur. Il s'agit du volet « possibilités » de la gestion des risques. Toutefois, dans les présentes lignes directrices, l'accent sera mis sur l'atténuation des incidences négatives des risques. Dans le cas des organisations qui disposent déjà d'un programme de GRE bien établi et qui s'orientent vers un état d'esprit d'optimisation des risques et des possibilités, se reporter aux lignes directrices sur la comptabilité de gestion intitulées *La courbe risque-valeur du CAM-I : Comprendre votre propension au risque en vue de créer de la valeur.*

3 CPA Canada, *RÉSILIENCE + ADAPTABILITÉ + INNOVATION = Durabilité. Le cadre RAID, reflet d'une nouvelle mentalité,* 2020.

Vue d'ensemble de la gestion des risques

Qu'est-ce que le risque?

Le mot *risque*, qui apparaît au milieu du XVII[e] siècle, a pour origine le mot italien *risco* qui, en gros, traduit la notion de *danger*.

La définition de risque utilisée pour les besoins des présentes lignes directrices est celle de la publication *Enterprise Risk Management* (2017) du COSO, à savoir [TRADUCTION] « la possibilité que des événements surviennent et aient une incidence sur la réalisation de la stratégie et des objectifs commerciaux ».

Le risque est évalué sous l'angle de l'incidence ou des répercussions d'un événement négatif ainsi que de la probabilité que cet événement se produise. Ces deux aspects sont fondamentaux lorsqu'il s'agit d'évaluer les risques et d'y répondre, parce que les organisations doivent se concentrer sur les risques dont les incidences sont plus importantes et dont la probabilité qu'ils surviennent est plus élevée, c'est-à-dire les risques critiques.

Qu'est-ce que la gestion du risque en entreprise?

La gestion des risques fait l'objet d'études depuis la fin de la Seconde Guerre mondiale[4]. Les organisations ont toujours géré des risques, parfois de façon inconsciente, implicite ou incohérente.

La gestion du risque en entreprise (GRE) ordonne simplement les pratiques de gestion des risques dans un cadre qui permet aux organisations de gérer les risques de manière plus cohérente et coordonnée.

Il est important de comprendre le *E* de GRE. La perspective de la GRE ne se limite pas aux risques financiers ou aux risques liés aux TI : elle englobe aussi la gestion des risques à l'échelle de l'entreprise ou de l'organisation. La GRE concerne tout le personnel et tous les secteurs et processus de l'organisation et se concentre sur les risques critiques. Il ne s'agit pas d'une gestion des risques ad hoc ou ponctuelle.

Cette approche peut sembler intimidante aux yeux d'organisations de plus petite taille, mais elle ne l'est pas vraiment. Les organisations de petite taille peuvent utiliser la même optique de gestion des risques que les organisations de grande taille lorsqu'elles planifient et examinent leurs stratégies et leurs objectifs généraux ainsi que dans le cadre de leurs activités quotidiennes. En effet, lorsque les petites et moyennes organisations développent ou améliorent leurs capacités de gestion des risques, elles ont l'avantage de pouvoir tirer parti de

4 Georges Dionne, « Risk Management: History, Definition, and Critique », *Risk Management and Insurance Review*, 2013.

pratiques opérationnelles existantes, de coûts de coordination moins élevés et de réseaux de communication interne plus efficaces.

[TRADUCTION] « La gestion du risque en entreprise débute par une simple question : quels sont les principaux risques qui peuvent nous empêcher d'accomplir notre mission? Toute cette question revient à la volonté de se pencher sur les grands risques. Et si vous pouvez intégrer cette volonté à votre culture, vous disposerez d'une capacité beaucoup plus grande pour comprendre les vulnérabilités auxquelles vous seriez autrement confronté sans les apprécier. »

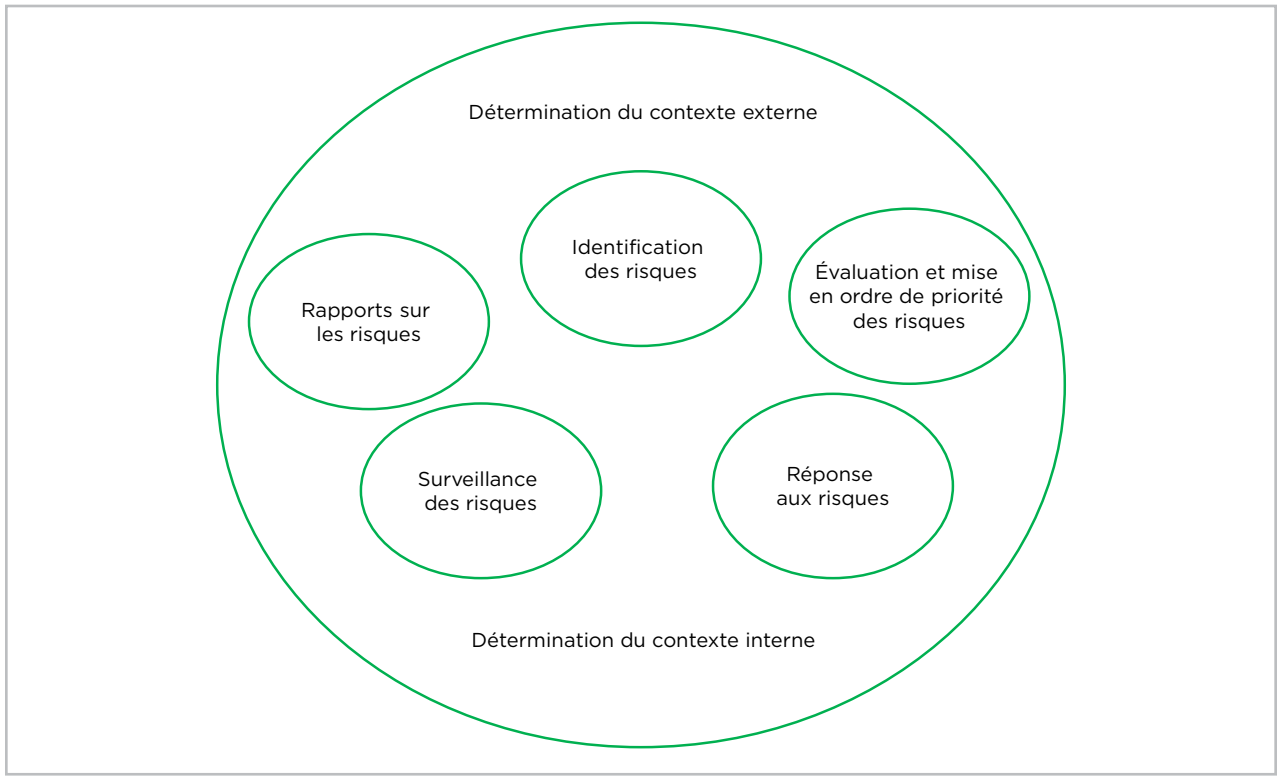
Enterprise Risk Management - Thomas Stanton, Université Johns Hopkins – Conférence TED – mars 2017

Par souci de simplicité et de cohérence, les présentes lignes directrices font référence au terme « gestion des risques », mais il convient de noter que la rigueur et les principes fondamentaux qui sous-tendent la gestion du risque en entreprise s'appliquent dans tous les cas mentionnés.

Quels sont les fondements de la gestion des risques?

Comme il a été indiqué, les organisations ont toujours géré les risques, mais le fait d'organiser et d'améliorer leurs pratiques en matière de gestion des risques leur permet de composer avec ces risques de manière plus efficace et efficiente. La figure 2 illustre une manière simple et pratique de conceptualiser et d'organiser ces pratiques[5].

FIGURE 2 – CADRE DE GESTION DES RISQUES



5 Ce cadre s'aligne sur les lignes directrices du COSO intitulées *Enterprise Risk Management – Integrating with Strategy and Performance* (2017), qui ont remplacé le cadre *Enterprise Risk Management – Integrated Framework,* et sur la norme ISO 31000 : 2018.

Les composantes du cadre de gestion des risques de la figure 2 sont définies comme suit :

Détermination des contextes externe et interne – Comprendre l'environnement dans lequel l'organisation exerce ses activités ainsi que les dynamiques externes (exigences de conformité réglementaires, attentes des clients et des parties prenantes, pressions concurrentielles et économiques, etc.) et internes (structure de gouvernance, culture, objectifs stratégiques, etc.).

Identification des risques – Comprendre tous les risques qui pourraient avoir une incidence sur l'organisation et qui pourraient l'empêcher d'atteindre ses objectifs stratégiques et opérationnels.

Évaluation et mise en ordre de priorité des risques – Déterminer le caractère critique des risques identifiés en estimant leur incidence et la probabilité qu'ils se produisent.

Réponse aux risques – Déterminer les réponses appropriées aux risques critiques en utilisant l'approche suivante, selon laquelle l'une ou l'autre des options est retenue :

- Contrôler le risque pour en réduire au minimum l'incidence ou la probabilité;
- Accepter le risque;
- Éviter le risque en ne cherchant pas à atteindre les objectifs sous-jacents;
- Transférer le risque (par exemple, grâce à une assurance).

Surveillance des risques – Passer en revue les risques critiques de façon continue à l'aide des indicateurs clés de risque (ICR) afin de s'assurer qu'ils n'augmentent pas à des niveaux inacceptables et que les contrôles fonctionnent comme prévu. Passer également en revue l'environnement en évolution pour détecter tout nouveau risque.

Rapports sur les risques – Communiquer toutes les informations pertinentes sur les risques (y compris le profil de risque de l'organisation) à toutes les principales parties prenantes, en temps opportun.

Processus

La mise en œuvre (ou l'amélioration) efficace d'un programme de gestion des risques comporte six étapes. Le calendrier de mise en œuvre du programme peut généralement varier de un à trois ans, selon les pratiques de gestion des risques existantes de l'organisation, sa culture du risque, sa taille et sa complexité.

Il n'est pas nécessaire de suivre ces étapes de manière séquentielle. En fait, il peut arriver que le champion de la gestion des risques d'une organisation réalise simultanément deux ou trois de ces étapes.

Étape 1

Mobiliser le conseil d'administration et/ou la haute direction – Afin d'assurer le succès du programme de gestion des risques, il est impératif que le conseil d'administration et/ou la haute direction en comprennent la valeur et qu'ils y adhèrent.

Étape 2

Établir les éléments de gouvernance des risques – Comme pour toute fonction organisationnelle, il est important de fournir certaines lignes directrices internes pour la gestion des risques. L'officialisation de la propension au risque, d'une politique de risque et des responsabilités en matière de risque fournit de telles indications.

Étape 3

Effectuer une évaluation des risques et des contrôles avec le conseil d'administration et/ou la haute direction – La direction doit comprendre les risques critiques de l'organisation et les gérer de manière appropriée.

Étape 4

Mobiliser le personnel – Comme les risques sont l'affaire de tous, il est important que l'ensemble du personnel comprenne les risques. La communication des priorités en matière de risque et l'obtention de commentaires sont essentielles pour gérer les risques de manière appropriée.

Étape 5

Accroître la valeur de la gestion des risques – Une fois que les pratiques fondamentales ont été établies ou améliorées, les organisations doivent continuer à surveiller les risques et envisager des mesures supplémentaires en matière de surveillance et de rapport.

Étape 6

Intégrer les pratiques de gestion des risques – La véritable valeur de la gestion des risques réside dans le fait qu'elle permet aux membres de l'organisation de participer aux principales décisions opérationnelles et stratégiques. L'alignement de la gestion des risques sur la planification et la stratégie permet d'atteindre cet objectif.

Principes directeurs

Les principes directeurs suivants contribuent à assurer le succès des six étapes du processus de mise en œuvre :

- Entamer les discussions au plus haut niveau, avec le conseil d'administration, la haute direction et les autres décideurs clés, afin de faciliter l'adhésion. Veiller à ce que ces parties soient considérées comme des promoteurs visibles.
- Mettre à profit les pratiques, les politiques et la documentation qui existent dans d'autres services de l'organisation (y compris l'audit interne, le service juridique, la conformité).
- Communiquer les avantages et les résultats attendus d'un programme de gestion des risques à l'échelle de l'organisation. Fournir le contexte (en expliquant en quoi la gestion des risques influe sur le travail quotidien des employés) contribue à obtenir l'adhésion des employés.
- Rechercher les premiers agents de changement au sein de l'organisation, et tirer parti de leur enthousiasme et de leurs liens internes pour établir des relations de confiance et de collaboration dans toute l'organisation.
- Désigner un champion de la gestion des risques qui jouit de la confiance du conseil d'administration et de la haute direction.
  - Dans une petite organisation, ce rôle est souvent rempli par le chef des finances, le chef de l'exploitation ou le propriétaire.
  - Dans les OSBL, ce rôle est souvent rempli par le directeur général.
  - Dans une organisation de taille moyenne, il faut tenir compte des points suivants lors de la nomination d'un champion de la gestion des risques :
    - Finance ou chef des finances – Cette fonction possède souvent une excellente orientation sur la surveillance interne et externe ainsi qu'une bonne compréhension des questions liées aux contrôles internes et à la gouvernance.
    - Planification ou stratégie d'entreprise – Cette fonction (si elle existe) est déjà responsable de la planification d'entreprise et peut soutenir une approche plus stratégique de la gestion des risques.
    - Auditeur interne ou auditeur en chef – Cette fonction est utilisée par certaines organisations pour élaborer les pratiques de gestion des risques, étant donné son expertise en matière de gouvernance et sa compréhension des systèmes, des processus opérationnels, des risques et des contrôles internes de l'organisation. Après leur élaboration, les pratiques de gestion des risques sont transmises au secteur le plus approprié de l'organisation.

Gestion des risques dans votre organisation – Le processus de mise en œuvre de la gestion des risques

Étape 1 – Mobiliser le conseil d'administration et/ou la haute direction

La première étape de la mise en œuvre d'un programme de gestion des risques consiste à obtenir l'adhésion du conseil d'administration et/ou de la haute direction et leur engagement continu envers ce programme.

Remarque : Ce ne sont pas toutes les organisations qui possèdent une structure comportant un conseil d'administration, un chef de l'exploitation ou une haute direction. Dans les présentes lignes directrices, les termes « conseil d'administration » et « haute direction » renvoient à la fonction d'une organisation qui est responsable des décisions organisationnelles et stratégiques importantes ainsi que de la surveillance des risques.

1.1 Cours de sensibilisation aux risques 101

Dans la plupart des cas, le conseil d'administration et/ou la haute direction n'ont pas une compréhension uniforme des risques auxquels l'organisation est confrontée et des stratégies de gestion des risques. Il est impératif de mettre tout le monde sur la même longueur d'ondes. La tenue d'une séance d'introduction de type « Gestion des risques 101 », comprenant une discussion interactive, permet à toutes les parties d'avoir une bonne compréhension des pratiques de gestion des risques.

Les sujets suivants devraient faire l'objet d'un examen et d'une discussion :

- la définition du risque et de la gestion des risques (c'est-à-dire le sens de chacun de ces termes au sein de l'organisation);
- les avantages d'un programme de gestion du risque en entreprise;
- des exemples courants et pertinents de risques et de leurs répercussions ultérieures qui se rapportent à l'industrie ou au secteur de services spécifique de l'organisation;
- les pratiques de gestion des risques généralement établies et la manière dont elles sont structurées dans un cadre;
- une « grille de classement des risques » et la façon dont elle relie les différentes étapes de la gestion des risques à l'intérieur du cadre (se reporter à la section 3.4 pour obtenir une description détaillée d'une grille de classement des risques);
- les responsabilités en matière de risque et les attentes en matière de gouvernance du conseil d'administration, de la direction et du personnel.

Exemple concret de la présentation d'une séance de sensibilisation à la gestion des risques au conseil d'administration de façon plaisante et interactive

Après avoir discuté des composantes du cadre de gestion des risques, les participants ont reçu une copie papier d'une grille de classement des risques et ont été invités à choisir un partenaire. Les questions suivantes ont été posées à chaque duo :

- Si vous partiez en randonnée, quels seraient les risques et à quel endroit les situeriez-vous dans la grille de classement des risques?
- Si vous envisagiez de mettre en place des contrôles supplémentaires pour chaque risque, à quoi le risque ressemblerait-il alors dans la grille de classement des risques?
- Quel est le niveau de risque acceptable, et quels sont les risques inacceptables?

Il y a eu beaucoup de bonnes interactions. La synthèse présentée au groupe a permis de s'assurer que les participants comprenaient les notions d'*incidence* et de *probabilité*, ainsi que la façon dont les risques se comparent entre eux et l'effet de la mise en œuvre de contrôles supplémentaires sur le niveau initial de risque inhérent.

1.2 Obtenir l'engagement du conseil d'administration et/ou de la haute direction

À la fin de la séance de sensibilisation, il est essentiel d'obtenir l'engagement du conseil d'administration à l'égard du programme de gestion des risques. Les participants doivent quitter la séance en ayant une compréhension de base des notions et des pratiques de gestion des risques. Il faut s'assurer ensuite que la gestion des risques fasse partie de l'ordre du jour du conseil d'administration, et il est impératif qu'elle y demeure tout au long de la mise en œuvre du programme de gestion des risques et jusqu'à ce que les activités atteignent une certaine stabilité.

Étape 2 – Établir les éléments de gouvernance des risques

Cette étape peut sembler arriver tôt dans la mise en œuvre d'un programme de gestion des risques, mais l'établissement des éléments de gouvernance tels que la propension au risque, la politique de risque et les responsabilités en matière de risque servira de base pour le reste du processus. Ces éléments de gouvernance des risques peuvent être revus et repensés tout au long de la mise en œuvre.

2.1 Déterminer la propension au risque

[TRADUCTION] « L'essentiel, c'est de prendre des décisions éclairées et intelligentes qui font intervenir le bon niveau de risque, ce risque étant justifié sur le plan des affaires et à d'autres égards. Les décideurs ont besoin d'indications pour savoir si ce qu'ils font (à savoir prendre un risque) cadre avec les souhaits de la haute direction et du conseil d'administration. »

Norman Marks on Governance, Risk Management and Audit, mars 2018

L'énoncé de la propension au risque définit le niveau de risque qu'une organisation est prête à accepter lorsqu'elle poursuit ses objectifs. Ainsi, [TRADUCTION] « définir la propension au risque, c'est évaluer tous les risques possibles avec lesquels une organisation doit composer, établir les limites des incidents acceptables et inacceptables, et créer les contrôles nécessaires du fait de ces limites[6] ».

Prenons cette notion dans le contexte d'un investissement financier : vous pouvez investir dans un projet risqué (ayant le potentiel de se traduire par des bénéfices majeurs ou de lourdes pertes) ou encore dans un projet sûr (dans le cas duquel le rendement serait moindre mais le risque de perdre de l'argent serait faible, voire nul). Le type d'investissement choisi dépendra de votre propension au risque.

Les énoncés de la propension au risque sont encore plus utiles lorsqu'ils intègrent la tolérance au risque. La tolérance au risque indique les seuils et les limites fixés pour la prise de risques. Elle permet aux organisations de mieux surveiller les risques. Les organisations sont ainsi alertées lorsqu'une activité ou un événement fait en sorte que le seuil de tolérance au risque est dépassé (ou est sur le point d'être atteint).

Les questions suivantes peuvent aider à amorcer les discussions d'une organisation au sujet de la propension au risque :

- Quelles activités sont absolument inacceptables et doivent être évitées?
- Qu'est-ce qui pourrait causer un tort irréparable à notre réputation?
- Qu'est-ce que nos clients, nos fournisseurs, les organismes de réglementation et les autres parties prenantes jugent trop risqué?
- Combien d'argent sommes-nous prêts à perdre par rapport au rendement que nous nous attendons à réaliser?
- Quel objectif, risque ou domaine d'activité serait assorti d'un niveau de propension au risque plus élevé ou plus faible qu'un autre?

Les énoncés de la propension au risque varient selon l'organisation, mais les exemples fournis au tableau 1 peuvent servir de ligne directrice.

6 Ariane Chapelle, *Operational Risk Management – Best Practices in the Financial Services Industry.*

TABLEAU 1 – EXEMPLES D'ÉNONCÉS DE LA PROPENSION AU RISQUE

Industrie ou secteur	Exemples d'énoncés de la propension au risque
Coopératives d'épargne et de crédit et autres services financiers[7]	La coopérative d'épargne et de crédit X est peu encline à accepter quelque concentration de risque importante que ce soit dans un secteur d'activité en particulier. Le niveau de tolérance au risque est alors jugé « faible ». La coopérative d'épargne et de crédit X a une tolérance légèrement plus élevée relativement à une défaillance de l'emprunteur dans le cas de prêts commerciaux. Le niveau de tolérance au risque est alors jugé « modéré ». La coopérative d'épargne et de crédit X ne souhaite pas faire face à une panne de système majeure. Le niveau de tolérance au risque est alors jugé « faible ».
Organismes de soins de santé[8]	L'organisme X s'efforcera de traiter tous les patients en salle d'urgence dans un délai de deux heures, et tous les patients dans un état critique dans un délai de 15 minutes. Toutefois, la direction accepte que, dans de rares cas (5 % du temps), certains patients dont la vie n'est pas menacée puissent ne pas recevoir de soins avant un délai pouvant aller jusqu'à quatre heures.
Organismes sans but lucratif[9]	Pour l'organisme X, les fonds de dotation trouvent un juste milieu entre la sécurité et des rendements potentiellement bas, et un potentiel de revenu plus élevé mais des risques plus importants. Quant à l'organisme X qui œuvre dans des régions dévastées par la guerre, il reconnaît qu'il fait courir à ses permanents et bénévoles des risques plus importants que ce qui serait acceptable dans leur pays d'origine, et prend les mesures nécessaires pour réduire ces risques au minimum.

2.2 Créer une politique de gestion des risques

Une politique de gestion des risques fournit des indications pour l'élaboration et la mise en œuvre de pratiques de gestion des risques à l'échelle de l'organisation. La politique et sa structure varient d'une organisation à l'autre, selon la nature de l'entreprise et de ses actifs.

Les composantes de base qui suivent doivent y être incluses :

- but ou objectifs de la politique;
- définition de « risque » et de « gestion des risques »;
- types de grands risques ou de catégories de risque qui touchent l'organisation;
- aperçu des pratiques de gestion des risques et des composantes du cadre;
- rôles et responsabilités en matière de gestion des risques (y compris pour le conseil d'administration et ses comités);

7 Société ontarienne d'assurance-dépôts, *Guide d'application : Gestion du risque d'entreprise*, janvier 2018.

8 Rittenberg et Martens, COSO, *Enterprise Risk Management – Understanding and Communicating Risk Appetite*, 2012.

9 Hugh Lindsay, CPA Canada, *20 Questions que les administrateurs d'organismes sans but lucratif devraient poser sur les risques*, 2009.

- références à d'autres politiques et/ou normes connexes.

La politique de gestion des risques devrait servir de politique globale encadrant les autres politiques et normes de l'organisation en matière de risque (par exemple, celles concernant la gestion de la continuité des activités ou la sécurité de l'information).

2.3 Définir les responsabilités en matière de gestion des risques

La définition des responsabilités en matière de gestion des risques contribue à ce que tous les membres de la direction et du personnel comprennent bien les obligations de reddition de comptes. À tout le moins, les responsabilités devraient être définies quant à ce qui suit :

- le conseil d'administration, pour son rôle de surveillance de la gestion des risques. Dans leur plus récente version, les normes ISO[10] et le cadre de GRE du COSO mettent l'accent sur la pression accrue qui est exercée sur les conseils pour qu'ils reconnaissent et assument leur rôle de surveillance;
- le comité de gestion des risques, pour son rôle de surveillance (si un tel comité existe);
- la haute direction, pour sa stratégie en matière de risque et son rôle de surveillance;
- les cadres hiérarchiques et les membres du personnel, pour les différents rôles qu'ils jouent en ce qui a trait aux pratiques de gestion des risques et aux réponses à l'égard des risques qui ont été approuvées (par exemple, contrôles internes), ainsi que pour les conseils pratiques qu'ils fournissent lors des examens.

Les petites organisations et les OSBL n'ont pas nécessairement une structure aussi détaillée, mais une distinction devrait tout de même y être faite entre le rôle de surveillance et celui de gestion.

Exemple concret de l'établissement d'un comité de gestion des risques au sein d'un cadre de gestion des risques dans une organisation de petite ou de moyenne taille

Une école indépendante a franchi plusieurs étapes au début de son processus de gestion des risques. Après avoir commencé par une séance de gestion des risques 101 qui traitait notamment de l'évaluation initiale des risques critiques avec lesquels l'école doit composer, il a été décidé de mettre sur pied un comité consultatif sur les risques (CCR).

Des membres du conseil d'administration et de la direction ont été choisis pour faire partie du CCR. Lors de l'une de ses premières réunions, le CCR a présenté et approuvé sa mission. Il s'est ensuite réuni pour examiner les risques critiques figurant dans le registre des risques de la direction. Peu après, la propension au risque a été établie. Un résumé des composantes clés du cadre de gestion des risques et des décisions prises a par la suite été présenté, lors d'une réunion rassemblant tous les membres du conseil. À ce stade, le CCR en est encore à ses débuts, mais sa valeur commence à être démontrée.

10 ISO 31000, *Management du risque – Lignes directrices*, fournit des principes, un cadre et des lignes directrices pour gérer toute forme de risque.

Étape 3 – Effectuer une évaluation des risques et des contrôles avec le conseil d'administration et/ou la haute direction

Après avoir obtenu l'adhésion du conseil d'administration et défini les éléments clés de la gouvernance, l'organisation est prête à mener une évaluation des risques et des contrôles avec le conseil d'administration et/ou la haute direction. Cette tâche globale comprend plusieurs des pratiques énoncées dans le cadre de gestion des risques (figure 2) : identifier les risques, évaluer les risques et les mettre en ordre de priorité selon leur ampleur ou leur importance, et déterminer la réponse appropriée.

Afin de se préparer, il est avantageux de dresser une liste des objectifs, des risques critiques et des programmes de contrôle interne existants de l'organisation. L'établissement d'une telle liste peut nécessiter des recherches externes.

Le tableau 2 présente des questions d'orientation de base sur la conduite d'une évaluation des risques et des contrôles.

TABLEAU 2 – QUESTIONS D'ORIENTATION AUX FINS DES DISCUSSIONS SUR LES RISQUES

Composante de risque	Questions d'orientation
Détermination des contextes externe et interne	Quels sont les contextes externe et interne de notre organisation?
Identification des risques	Quels sont nos objectifs stratégiques? Quels risques peuvent avoir des répercussions sur nous et nuire à l'atteinte de nos objectifs stratégiques?
Évaluation et mise en ordre de priorité des risques	Parmi les risques pouvant avoir des répercussions sur nous, quels sont les plus critiques?
Réponse aux risques	Quelles mesures prenons-nous pour gérer ces risques critiques? Que devrions-nous faire d'autre?

Les réponses à ces questions peuvent être résumées au moyen d'une grille de classement des risques, de façon à fournir en temps réel un aperçu visuel des risques critiques.

Des précisions supplémentaires sur chaque composante de risque présentée au tableau 2 sont fournies ci-dessous.

3.1 Déterminer les contextes externe et interne

L'objectif de cette étape est de veiller à ce que le conseil d'administration et/ou la haute direction comprennent parfaitement les facteurs externes et internes qui déterminent la nature des risques que l'organisation devra gérer.

Le modèle PESTEL peut aider une organisation à analyser et à comprendre ses facteurs macroenvironnementaux, c'est-à-dire son contexte externe. Il résume les facteurs externes qui peuvent influer sur une organisation : **p**olitiques, **é**conomiques, **s**ocioculturels, **t**echnologiques, **e**nvironnementaux et **l**égaux.

Les catégories de facteurs internes pouvant être utilisées pour établir le contexte interne d'une organisation sont la gouvernance, le capital, le personnel, les processus et la technologie.

La compréhension des facteurs externes et internes peut également aider l'organisation à affiner ses éléments de gouvernance du risque (propension au risque, politique de gestion des risques et responsabilités en matière de risque).

3.2 Identifier les risques

Une fois que l'organisation a déterminé ses contextes interne et externe, elle est prête à discuter des risques auxquels elle est exposée.

L'objectif de l'identification des risques consiste à cerner et à comprendre tous les risques réels ou potentiels qui pourraient avoir une incidence sur l'organisation et l'empêcher d'atteindre ses objectifs stratégiques et opérationnels.

Le point de départ, avant même de procéder à l'identification des risques, est la compréhension et l'énoncé des objectifs. Il est difficile de déterminer les risques de manière adéquate si les objectifs de l'organisation ne font pas consensus ou ne sont pas bien compris.

Les questions d'orientation (tableau 2) et les exemples de risques auxquels les petites et moyennes organisations sont couramment exposées (tableau 3, ci-dessous) peuvent aider les personnes concernées à élaborer une liste préliminaire de risques.

TABLEAU 3 – EXEMPLES DE RISQUES ET D'ÉVÉNEMENTS

Industrie ou secteur	Types de risques
Non propres à une industrie – petites et moyennes organisations[11,12]	• Risques posés par les clients, les concurrents, les fournisseurs ou le personnel • Risques posés par les locaux, l'emplacement ou les technologies de l'information de l'entreprise • Risques posés par les opérations financières, le marché ou l'économie • Départ inattendu d'un partenaire d'affaires ou d'un employé clé • Menaces d'atteinte à la réputation et au capital de sympathie

11 CPA Australia, *Risk Management Guide to Small and Medium Sized Businesses*, 2009.

12 D'autres risques peuvent se poser : flux de trésorerie et insolvabilité, succession de l'entreprise familiale, protection de la propriété intellectuelle, cyberattaques, fraude, chaîne d'approvisionnement et durabilité, fiscalité (Accountancy Europe Briefing Paper VIEWS, *SME Risk Management. How can your accountant help?*).

Industrie ou secteur	Types de risques
Coopératives d'épargne et de crédit[13]	• Risque stratégique : mise en œuvre de stratégies, renseignements démographiques sur les sociétaires, concurrence • Risque de crédit : défaillance, concentration des prêteurs • Risque financier : liquidité, gestion du capital • Risque opérationnel : technologies de l'information, sécurité de l'information, impartition, fraude, personnel, cybermenaces • Risque de conformité : réglementation (blanchiment de capitaux, etc.)
Fabrication[14]	• Retards dans la chaîne d'approvisionnement et ennuis avec les fournisseurs tiers • Erreurs et omissions ou pièces défectueuses • Défaillance de l'équipement • Cybermenaces
Organismes sans but lucratif[15]	• Perte d'une source importante de financement, projets de collecte de fonds infructueux • Réduction de la valeur marchande des placements, fraude interne ou externe • Échec d'un projet ou d'une initiative stratégique • Non-pertinence parce que les programmes ou les services ne sont plus populaires ou originaux • Atteinte à la réputation (inconduite ou abus sexuel véritable ou présumé par un employé ou un bénévole, etc.)

3.3 Évaluer les risques et les mettre en ordre de priorité

Une fois les risques identifiés, ils ne peuvent et ne doivent pas tous être atténués. Les organisations doivent attribuer judicieusement les ressources, afin que l'investissement soit justifié par une amélioration du résultat. Les risques doivent donc être catégorisés en fonction de leur ampleur ou de leur importance, de façon à ce qu'ils fassent l'objet d'un niveau approprié d'attention et de surveillance. Cette approche permet d'optimiser la valeur de la gestion des risques pour l'organisation.

Pour évaluer et mettre en ordre de priorité les risques importants, les organisations estiment l'incidence de ces risques et la probabilité qu'ils se matérialisent.

13 Société ontarienne d'assurance-dépôts, *Guide d'application : Gestion du risque d'entreprise*, janvier 2018.

14 Northbridge Assurance, *Détecter les risques cachés liés à la fabrication*, juillet 2017.

15 Hugh Lindsay, CPA Canada, *20 Questions que les administrateurs d'organismes sans but lucratif devraient poser sur les risques*, 2009.

L'*incidence* de la survenance d'un événement peut être définie non seulement en termes financiers, mais aussi dans la perspective de la réglementation et de la réputation. Le tableau 4 présente un exemple d'échelle des niveaux d'incidence.

TABLEAU 4 – EXEMPLES DE NIVEAUX D'INCIDENCE D'UN ÉVÉNEMENT

Niveau	Incidence financière	Incidence réglementaire	Incidence sur la réputation
Extrême	Perte de financement ou de revenus annuels de plus de 20 %	Perte d'autorisation réglementaire d'exercer ses activités	Couverture médiatique négative à long terme, perte colossale de parts de marché
Majeur	Perte de financement ou de revenus annuels de 10 % à 20 %	Amendes réglementaires majeures	Couverture médiatique négative importante, fortes répercussions sur les parts de marché
Modéré	Perte de financement ou de revenus annuels de 5 % à 10 %	Avertissement réglementaire officiel écrit	Couverture médiatique modeste et de courte durée
Mineur	Perte de financement ou de revenus annuels de 5 %	Avertissement réglementaire verbal	Couverture médiatique mineure

La *probabilité* qu'un événement survienne est généralement définie en fonction de la mesure dans laquelle il est susceptible de se matérialiser et de la fréquence à laquelle il survient. L'évaluation de la probabilité constitue, jusqu'à un certain point, un jugement et peut se fonder sur des expériences passées ou sur des événements survenus dans des organisations similaires. L'horizon temporel peut varier selon l'organisation ou l'industrie (l'horizon de base est de 10 ans). Le tableau 5 présente un exemple d'échelle des niveaux de probabilité.

TABLEAU 5 – EXEMPLES DE NIVEAUX DE PROBABILITÉ DE LA SURVENANCE D'UN ÉVÉNEMENT

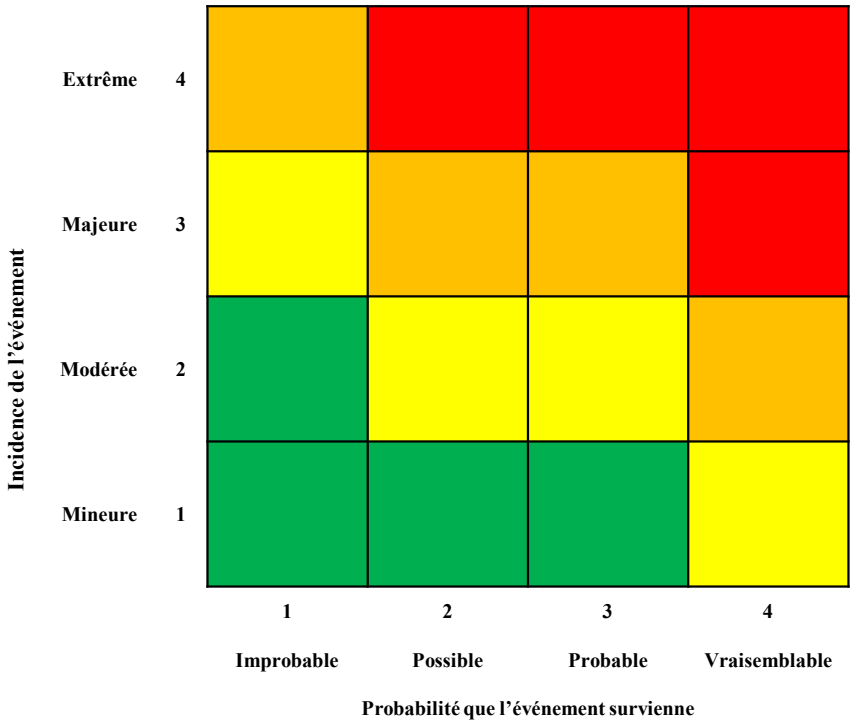
Niveau	Probabilité	Fréquence
Vraisemblable	Plus de 66 % dans une année	L'événement surviendra probablement une ou plusieurs fois dans la prochaine année
Probable	De 33 % à 66 % dans une année	L'événement est susceptible de survenir une fois au cours des 5 prochaines années
Possible	De 5 % à 33 % dans une année	L'événement est susceptible de survenir une fois au cours des 5 à 10 prochaines années

Niveau	Probabilité	Fréquence
Improbable	Moins de 5 % dans une année	L'événement est rare et est susceptible de survenir une fois au cours des 10 prochaines années ou plus

3.4 Représenter les évaluations dans une grille de classement des risques

Une fois que les organisations ont déterminé l'incidence des risques et la probabilité qu'ils se matérialisent, elles peuvent les représenter dans une grille de classement des risques. Cette grille illustre les zones où se recoupent l'incidence et la probabilité associées à chaque risque (voir l'exemple à la figure 3, ci-après). Il s'agit d'un excellent outil qui permet au conseil d'administration et/ou à la haute direction de visualiser le niveau de chacun des risques que l'organisation a identifiés.

FIGURE 3 – GRILLE DE CLASSEMENT DES RISQUES



Les niveaux d'incidence et de probabilité associés à un risque permettront de déterminer dans quelle cellule de la grille le risque en question se situe. Chaque cellule a une couleur (vert, jaune, orange ou rouge) qui représente le rapport entre les niveaux d'incidence et de probabilité et la propension au risque de l'organisation. Les risques qui se situent dans la zone verte sont considérés comme faibles et doivent simplement être surveillés. Plus haut dans la grille, les risques se situant dans une cellule jaune ou orange sont plus critiques et doivent être

évalués avec soin pour que la meilleure réponse soit déterminée à leur égard. Les risques se trouvant dans la zone rouge indiquent que le seuil de propension au risque de l'organisation est dépassé et doivent faire l'objet de mesures immédiates.

Notons que certaines organisations utilisent une grille de classement des risques de 5 éléments par 5 éléments, ce qui peut être tout aussi efficace. Les couleurs des cellules peuvent également varier à la discrétion de l'organisation.

3.5 Répondre aux risques critiques

Une fois que la grille de classement des risques a été mise en place, l'organisation est prête à déterminer comment répondre le plus adéquatement possible aux risques critiques et s'assurer que la réponse concorde avec la propension au risque de l'organisation. L'une des réponses possibles consiste à atténuer le risque en appliquant une forme de contrôle appropriée. Éviter le risque, l'accepter ou le transférer (par exemple, grâce à une assurance) peuvent constituer d'autres options.

Si un risque avoisine ou dépasse le seuil de propension au risque de l'organisation, celle-ci doit mettre en œuvre au moins une de ces réponses jusqu'à ce que le niveau résiduel d'un risque en particulier soit réputé cadrer avec la propension au risque de l'organisation. Les réponses aux risques doivent faire l'objet d'une surveillance continue (et leur efficacité doit être évaluée) pour veiller à ce que les risques soient traités de manière appropriée.

Les résultats estimés des réponses peuvent être représentés dans la grille de classement des risques, qui devrait montrer une diminution du niveau de risque par rapport au niveau initial.

3.6 Utiliser un registre des risques pour consigner les informations sur les risques

Au moment d'identifier un risque, de le classer en fonction de son niveau et d'y répondre, le fait de consigner les informations sur ce risque dans un registre permet de les conserver aux fins de la surveillance et des rapports futurs.

Le registre des risques peut servir à résumer les objectifs de l'organisation, les risques identifiés, les niveaux de risque, les contrôles internes appropriés et les plans d'action établis à l'égard des risques critiques. Un registre des risques peut être créé à l'aide d'une simple feuille de calcul, comme il est illustré au tableau 6.

TABLEAU 6 – EXEMPLE DE REGISTRE DES RISQUES

Risque	Catégorie de risque	Souscatégorie	Description du risque	Risque inhérent*			Réponse au risque	Programme de contrôle	Risque résiduel**			Mesures supplémentaires		
				Niveau d'incidence	Niveau de probabilité	Niveau de risque inhérent			Niveau d'incidence	Niveau de probabilité	Niveau de risque résiduel	Mesure spécifique	Responsabilité	Échéancier
1	Opérationnel	Risque lié aux TI	Piratage informatique	Extrême	Probable	Critique	Atténuation	Normes ISO pour les TI	Majeur	Possible	Majeur	• Examiner les pratiques novatrices en matière de sécurité informatique, comme le pot de miel ou leurre		
2	Opérationnel	Impartition	Accords conclus avec des tiers et contenant des informations sur la lutte contre le blanchiment d'argent, qui ont été égarés	Majeur	Probable	Majeur	Atténuation	Mettre en œuvre les normes relatives à la lutte contre le blanchiment d'argent de la SOAD	Modéré	Probable	Modéré	• Organiser des audits de tiers • Examiner les informations confidentielles pour déterminer si certaines peuvent être retenues		
3	Stratégique	Satisfaction des sociétaires	Faible satisfaction des clients	Majeur	Probable	Majeur	Atténuation	S'efforcer de toujours connaître ses clients	Majeur	Possible	Majeur	• Réexaminer en permanence sa stratégie et celle de la concurrence • Se concentrer sur des créneaux spécifiques sur le marché		
4	Opérationnel	Personnel	Départ d'éléments de valeur	Majeur	Probable	Majeur	Atténuation	Programme d'attraction et de fidélisation des RH	Modéré	Possible	Modéré	• Créer un bassin de candidats qualifiés • Mettre en place de nouvelles initiatives de formation croisée		

*Le **risque inhérent** est le niveau de risque actuel en l'absence d'une réponse au risque.

Le **risque résiduel est le niveau de risque qui demeure après la réponse de la direction au risque.

Étape 4 – Mobiliser le personnel

> « Il faut se poser la question suivante : *qui affirme que ces risques sont les risques les plus importants et quel est le parti pris ou la perspective naturelle de cette personne?* À moins d'avoir les points de vue d'un échantillon représentatif des différents niveaux hiérarchiques d'une grande organisation, par opposition aux seuls points de vue de la haute direction, vous n'aurez pas une bonne compréhension des risques réels auxquels l'organisation fait face. »
>
> Robert McFarlane, administrateur de sociétés et ancien vice-président directeur et chef des finances, TELUS[16]

À la suite des discussions et des évaluations des risques au sein du conseil d'administration et/ou de la haute direction, la tâche consiste à présenter les discussions concernant la gestion des risques au reste de l'organisation. L'objectif est de sensibiliser l'organisation aux pratiques de gestion des risques, de façon à obtenir les points de vue de tous les membres du personnel et à favoriser l'adhésion.

4.1 Favoriser la sensibilisation et la mobilisation au sein de l'organisation

Pour de nombreuses petites et moyennes organisations, il devrait y avoir plusieurs occasions de mener des évaluations des risques à des niveaux inférieurs de l'organisation et de créer des registres des risques supplémentaires par service.

Ces évaluations des risques à des niveaux inférieurs peuvent mettre au jour des risques qui n'étaient pas pris en compte au niveau du conseil d'administration ou de la haute direction, ce qui est compréhensible, étant donné que ceux-ci envisagent le risque de façon plus globale ou stratégique. Les secteurs d'exploitation, quant à eux, examinent le risque à un niveau pratique et concret. Ces deux points de vue sont essentiels à l'établissement d'un profil de risque complet de l'organisation.

Certaines organisations peuvent initialement estimer qu'il n'est pas nécessaire de procéder à des évaluations des risques à des niveaux inférieurs, et il se peut que ce soit tout à fait correct. Toutefois, il se pourrait que des informations importantes sur les risques passent inaperçues à un niveau inférieur et que le moral des membres du personnel s'en trouve affecté, puisque leurs points de vue et leurs idées ne seraient pas sollicités.

Au moment de sensibiliser et de mobiliser l'ensemble de l'organisation, il est important de gagner la confiance de tout le personnel. De plus, il est essentiel de comprendre et de reconnaître les incidences de ce processus sur le plan humain, notamment en appliquant certaines pratiques de base de gestion du changement[17].

16 CPA Canada, *L'état actuel de la gestion des risques d'entreprise au Canada*, 2016

17 Se reporter aux lignes directrices sur la comptabilité de gestion intitulées *Engaging Change – Using a Learning Approach to put the Humanity back into Change Management*, et ***Gestion du changement organisationnel – Le modèle de parcours du changement pour favoriser la durabilité organisationnelle***.

Exemple concret d'une évaluation des risques effectuée à des niveaux inférieurs de l'organisation et d'une manière d'inspirer confiance au sein d'unités individuelles

Dans une organisation, l'équipe de gestion des risques a offert des séances de formation pratique qui ont été intégrées à des séances sur l'évaluation des risques. Tout au long de ces séances, l'équipe de gestion des risques a posé des questions et saisi la position du secteur de l'organisation en matière de risque. Dans le cadre de ce processus, les réponses des différents secteurs de l'organisation ont été remises en cause, en particulier lorsqu'elles concernaient des restrictions touchant le financement. L'équipe de gestion des risques a reconnu que le financement constituait un défi – l'équipe a traité le financement comme une cause profonde potentielle plutôt que comme un risque critique, afin d'orienter la conversation dans une direction précise.

L'équipe de gestion des risques a également travaillé à renforcer le capital social et la confiance en aidant les secteurs d'activité à surmonter les problèmes et les défis avec lesquels ils devaient composer, allant ainsi au-delà des simples fonctions de gestion des risques. L'équipe de gestion des risques a terminé certains travaux et mis certains secteurs en contact avec d'autres disposés à les aider, ce qui a contribué à l'établissement de relations solides. La gestion des risques est plus souvent une affaire de gestion des relations que de science exacte.

4.2 Offrir de la formation continue

La sensibilisation et la mobilisation de l'organisation quant aux notions et aux pratiques de gestion des risques peuvent également passer par la mise en place de séances de formation continue à l'intention de la direction et du personnel.

La formation pratique en gestion des risques peut se faire lors des séances sur l'évaluation des risques. L'intégration des mesures ou des pratiques de gestion des risques dans des programmes de formation peut permettre à la direction et au personnel de mieux comprendre les notions concernées. La formation en gestion des risques peut également s'inscrire dans le cadre de séances de suivi individuelles.

Les pratiques de gestion des risques existantes, notamment les approbations annuelles liées au code de déontologie et les formations sur la confidentialité, la sécurité, le harcèlement et la fraude, peuvent être considérées comme des formations en gestion des risques. Certaines organisations tiennent des réunions du personnel consacrées à la gestion des risques. Elles y abordent des sujets liés à la gestion des risques qui favorisent le dialogue et les discussions interactives et qui véhiculent des connaissances approfondies sur la résolution de problèmes grâce à l'expérience partagée.

Étape 5 – Accroître la valeur de la gestion des risques

Comme dans le cas de n'importe quel autre processus organisationnel, l'amélioration ou l'affinage des pratiques de gestion des risques contribuera à permettre à une organisation en évolution de continuer à répondre à ses besoins changeants.

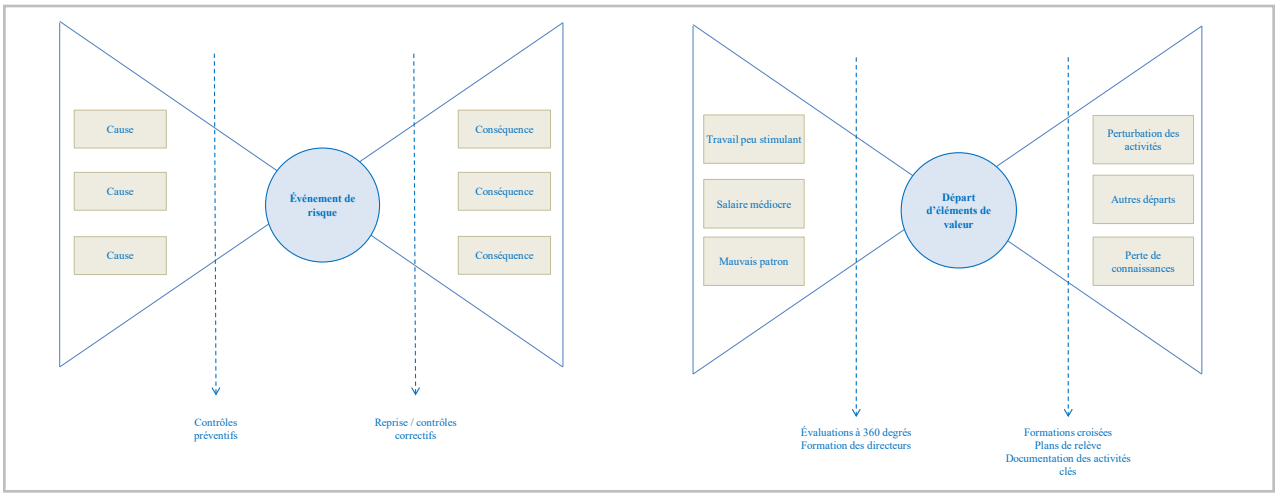
L'examen et la mise à jour des diverses composantes du cadre de gestion des risques devraient se faire au moins une fois l'an.

5.1 Exécuter une analyse des causes profondes – La méthode nœud papillon

La méthode nœud papillon (voir la figure 4) est un outil utile pour identifier les risques, les comprendre et les classer en fonction de leur niveau. Il s'agit d'une représentation visuelle de la relation entre un événement de risque et ses causes et conséquences.

Une fois que les causes et les conséquences ont été traitées et documentées, l'organisation peut établir des contrôles qui aideront à prévenir la survenance d'un événement de risque ou à en réduire au minimum les répercussions, de façon à ce que le seuil de propension au risque ne soit pas dépassé.

FIGURE 4 – MÉTHODE NŒUD PAPILLON ET EXEMPLE



Selon un exemple tiré de l'ouvrage d'Ariane Chapelle intitulé *Reflections on Operational Risk Management*, une société identifie le départ d'éléments de valeur comme un événement de risque. Il s'agit de la première étape de l'analyse selon la méthode nœud papillon, qui consiste à identifier l'événement de risque, soit le point central du nœud papillon. Une fois l'événement de risque identifié, il faut effectuer ce qui suit :

- En commençant par l'analyse des causes profondes, soit le côté gauche du nœud papillon, identifiez les causes profondes de l'événement de risque (peu de mandats stimulants, mauvais gestionnaire, etc.). Voyez comment atténuer le risque. Par exemple, les contrôles préventifs à envisager comprendraient la mise en place d'évaluations à 360 degrés et/ou de formations ciblées à l'intention de la direction.

- Ensuite, au chapitre des conséquences majeures, soit le côté droit du nœud papillon, le départ d'éléments de valeur pourrait se traduire par une énorme perte de connaissances pour l'organisation. Voyez comment réduire au minimum cette perte. Par exemple, les contrôles correctifs à envisager comprendraient le déploiement d'une formation continue interservices et la documentation des processus et des procédures clés.

5.2 Développer les capacités de surveillance du risque – Indicateurs clés de risque

L'objectif de cette étape est de veiller à ce que les risques critiques n'augmentent pas à des niveaux inacceptables (au-delà de la propension au risque de l'organisation) et à ce que les réponses mises en œuvre (par exemple, les contrôles internes) fonctionnent comme prévu. Cela peut se faire par l'établissement d'indicateurs clés de risque (ICR) pour tous les risques critiques.

Les ICR, qui sont des mesures liées à un risque en particulier, indiquent si les réponses mises en œuvre fonctionnent comme prévu ou non. Ils peuvent constituer des prédicteurs des risques ou des événements importants qui peuvent nuire à l'organisation. À ce titre, les ICR sont alignés sur les énoncés de la propension au risque et sur les niveaux de tolérance au risque.

De nombreuses organisations disposent de certains types d'indicateurs pouvant servir d'ICR (par exemple, mesures de sécurité, départs volontaires, révisions des mandats d'audit). L'un des principaux défis consiste à développer des ICR prédictifs qui fournissent une indication de la possibilité que des événements défavorables surviennent dans l'avenir. Une combinaison d'ICR de suivi / témoins et d'ICR prédictifs/guides devrait être mise au point.

TABLEAU 7 – EXEMPLES D'INDICATEURS CLÉS DE RISQUE (ICR)[18]

Nature du risque	Facteur de risque clé	Description de l'ICR	Limites (tolérance)		
Sécurité de l'information : données sensibles compromises	Intrusion frauduleuse (piratage, hameçonnage)	Nombre de tentatives d'intrusion externes fructueuses	0	1	>1
		Nombre de personnes ayant un profil inapproprié d'accès au système	0	1	>1
Conformité réglementaire : non-conformité aux règlements	Nouveaux règlements	Nombre de nouveaux problèmes réglementaires considérés comme étant « à risque élevé »	< 2	de 2 à 5	> 5

18 Comprend des références au guide *Key Risk Indicators* de l'Institute of Operational Risk, 2010.

Nature du risque	Facteur de risque clé	Description de l'ICR	Limites (tolérance)		
Personnel : baisse de motivation et de productivité	Effectifs dont la productivité est instable	Départs volontaires d'employés hautement performants	0 %	de 0 % à 5 %	> 5 %
	Effectifs peu motivés	Résultats des sondages de satisfaction des employés et des évaluations à 360 degrés des superviseurs et des directeurs	> 80 %	de 60 % à 80 %	< 60 %
Fidélisation de la clientèle : perte de parts de marché	Plaintes de clients quant à la qualité des produits	Tendances concernant la nature et le volume des plaintes des clients	de 0 à 2	de 2 à 4	> 4
Disponibilité des systèmes : systèmes informatiques essentiels non disponibles	Pannes de système	Pourcentage de temps où les systèmes essentiels sont disponibles au cours du mois et tendance mensuelle	> 99,75 %	de 99,0 % à 99,75 %	< 99,0 %
Contrôles internes	Problèmes internes ou externes liés à l'audit	Nombre de constatations majeures découlant de l'audit, note d'audit	de 0 à 1	de 1 à 2	> 2

Dans l'exemple du départ d'éléments de valeur présenté à la section 5.1 sur la méthode nœud papillon, un ICR utile pour les « conséquences » serait le pourcentage de formations croisées suivies ou de plans de relève mis en place. S'agissant des « causes », il serait pertinent de développer un ICR correspondant au pourcentage de mauvaises évaluations à 360 degrés d'un directeur par rapport au total des évaluations.

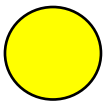
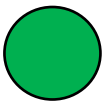
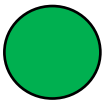
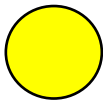
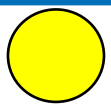
5.3 Élaborer des rapports sur les risques – Tableaux de bord de la gestion des risques

Il est important de communiquer à toutes les parties prenantes pertinentes, en temps opportun, le profil de risque de l'organisation relativement à ses objectifs stratégiques et opérationnels et à sa propension au risque. Une fois que le conseil d'administration et la haute direction ont bien compris les risques critiques, il est important de faire rapport régulièrement sur la façon dont l'organisation s'y prendra pour gérer ces risques. Dès lors que les pratiques de gestion des risques ont été améliorées et qu'elles permettent de produire des informations supplémentaires de qualité, les rapports sur les risques peuvent être affinés.

En plus des risques critiques communiqués à l'échelle de l'organisation, un sommaire complet des objectifs et des risques de même qu'une opinion sur la manière dont ils sont gérés peuvent être présentés au conseil d'administration et à la haute direction, de façon périodique (par exemple, sur une base trimestrielle, semestrielle ou annuelle, selon les exigences du conseil ou des parties prenantes). Cette façon de faire aide à assurer la mobilisation et l'engagement continus envers la gestion des risques.

Les rapports ou les tableaux de bord sur les risques devraient comprendre un sommaire des objectifs stratégiques, des risques critiques et des ICR, de même qu'un compte rendu éclairant et détaillé. Le niveau de précision du rapport peut s'accroître au fil du temps.

TABLEAU 8 – EXEMPLE DE RAPPORT SUR LES RISQUES

Stratégie	Risques		Évaluation du risque		Capacité à gérer le risque	Principal plan d'atténuation et état de la situation	Perspectives liées au risque	Certitude d'atteindre l'objectif stratégique
	Type	Énoncé du risque	Trimestre actuel	Trimestre précédent				
Stratégie n° 1	Opérationnel - RH	Brève description expliquant pourquoi il s'agit d'un risque / d'une possibilité pour les objectifs opérationnels de la division				Bref résumé des principaux plans d'atténuation pour traiter le risque élevé		
	Opérationnel – TI	Brève description expliquant pourquoi il s'agit d'un risque / d'une possibilité pour les objectifs opérationnels de la division				Bref résumé des principaux plans d'atténuation pour traiter le risque élevé		
	Nouveaux risques							
	Opérationnel – RH	Nouveaux risques détectés grâce à l'analyse de l'environnement		-		Résumé des plans de la direction pour continuer à les surveiller et à éventuellement s'y préparer		

Étape 6 – Intégrer les pratiques de gestion des risques

Pour intégrer la gestion des risques dans la culture de l'organisation, il faut notamment se poser certaines questions liées aux risques lorsqu'il s'agit d'élaborer des stratégies, d'évaluer la faisabilité de la mise en place de nouveaux produits ou services, ou encore de bonifier la gamme de produits offerts par la société.

Exemple concret de l'intégration des pratiques de gestion des risques dans les activités quotidiennes d'un organisme sans but lucratif

Dans une grande ville canadienne, lorsque des sans-abri reçoivent des soins en salle d'urgence, ils obtiennent ensuite leur congé et sont envoyés au refuge le plus proche par le personnel de l'hôpital. Le gestionnaire des services qui s'occupe des refuges a pour mission de soutenir les sans-abri dans leur recherche d'un logement sûr et stable. Il est d'autant plus difficile de remplir cette mission que les personnes concernées ont des besoins complexes en matière de soins de santé.

Afin de mieux gérer le risque de se retrouver submergé par un trop grand nombre de sans-abri ayant des besoins complexes, le gestionnaire des services a établi (et s'est vu approuver) une « propension au risque », à savoir un ensemble de critères à appliquer lorsque les fournisseurs de soins de santé procèdent à l'admission de clients et mettent au point un plan de sortie de l'hôpital. La mise en application de ces critères a donné lieu à une meilleure compréhension, par les parties prenantes du système de santé, des capacités du réseau de refuges et, plus important encore, à une amélioration des services et des soins fournis aux personnes dans le besoin.

6.1 Aligner les risques sur la planification et la stratégie

Les risques sont des incertitudes qui peuvent prendre la forme d'événements ayant une incidence sur la capacité de l'organisation à réaliser ses objectifs stratégiques. Il est donc impératif d'arrimer clairement les processus de planification stratégique aux processus de gestion des risques.

Au cours des séances annuelles sur la stratégie et la planification, les organisations peuvent soulever les questions suivantes afin d'alimenter la conversation :

- Quels sont les risques associés à la mise en place de stratégies inadéquates? Que faisons-nous pour nous assurer que nos stratégies sont optimales?
- Quels sont les risques associés à une mauvaise compréhension de nos concurrents? Que faisons-nous pour remédier à la situation?
- Quels sont les risques qui se posent si nous ne disposons pas des capacités nécessaires pour mettre en œuvre correctement nos stratégies? Que faisons-nous pour répondre à ces risques?
- Quelle est la pire chose qui puisse arriver en ce qui a trait à notre réputation?

La mise en place d'un processus d'approbation pour les nouveaux produits et services est une autre façon d'aligner les risques sur la stratégie. Ce processus peut notamment consister en une évaluation éclair des risques pour chaque nouveau produit ou service offert. La haute direction se penche sur tous les risques pertinents et les approuve s'ils concordent avec la propension au risque de la société.

[TRADUCTION] « Le risque et la stratégie sont les piliers d'une entreprise; ils ont le même pouvoir de créer ou de détruire de la valeur. Ils nécessitent le même niveau de talent et d'attention. Les priorités de la direction et la surveillance exercée par le conseil d'administration doivent refléter cette réalité. »

Olivia F. Kirtley, administratrice, U.S. Bancorp, Papa John's International, Randgold Resources, et présidente du Jury d'examen de l'AICPA[19]

6.2 Analyse des hypothèses les plus défavorables

La simulation de crise (ou l'analyse des hypothèses les plus défavorables) est une technique de gestion des risques qui permet d'évaluer les répercussions potentielles d'un événement sur la situation financière d'une organisation. De nombreuses organisations réalisent des simulations de crise pour s'assurer qu'elles sont prêtes à faire face à des événements internes ou externes inattendus qui pourraient perturber considérablement leurs activités et entraîner des pertes financières majeures. Du point de vue de la gestion des risques, la probabilité qu'un événement de risque tel que la pandémie de 2019 se produise est faible. Toutefois, si l'événement de risque se matérialise, il aura une incidence néfaste extrême sur la capacité de l'organisation à générer et à maintenir ses flux de trésorerie et à poursuivre ses activités. Si on se reporte à la grille de classement des risques (voir la **figure 3**, à la section 3.4), un risque extrême de ce type se situerait dans la cellule correspondant à un scénario improbable ayant une incidence extrême.

Le conseil d'administration et/ou la haute direction, en collaboration avec les experts des domaines pertinents, doivent prendre part à l'élaboration des scénarios potentiels et à l'identification des répercussions les plus défavorables pour les activités d'une organisation. Il est important que les participants mettent de côté l'idée qu'un événement « ne pourrait jamais se produire », et qu'ils se demandent plutôt ce qui arriverait si cet événement se matérialisait bel et bien. Les catastrophes naturelles, les conditions météorologiques extrêmes, les guerres commerciales mondiales, les pandémies et les fraudes à grande échelle découlant de cyberattaques sont des exemples d'hypothèses les plus défavorables[20].

Au moment d'évaluer les hypothèses les plus défavorables, le recours à la méthode nœud papillon (voir la **figure 4**, à la section 5.1) peut faciliter la discussion concernant les conséquences possibles de chaque hypothèse. L'équipe devrait se pencher sur toutes les causes possibles de chacun des événements les plus défavorables, évaluer si les contrôles et les processus en place devraient être renforcés, et déterminer s'il est nécessaire de mettre en œuvre des contrôles,

19 CIMA AICPA, *Enterprise Risk Oversight: A Global Analysis*, septembre 2010.

20 Rapport sur les risques mondiaux 2020 du Forum économique mondial.

des plans, des processus et des systèmes de prévention supplémentaires (par exemple, pour la continuité des activités, la reprise après sinistre, la préparation aux situations d'urgence, les systèmes de gestion des urgences, la gestion de crise). Dans l'éventualité où un risque extrême se matérialiserait, ces plans peuvent s'avérer avantageux, car ils permettent notamment :

- de répondre aux préoccupations des employés de l'organisation en matière de santé et de sécurité;
- de veiller à ce que les processus opérationnels cruciaux continuent de fonctionner efficacement;
- de maintenir la viabilité financière si l'hypothèse la plus défavorable devait se concrétiser.

La planification à l'aide de scénarios[21] est un autre outil de gestion qui peut être exploité pour la prise de décisions organisationnelles dans des contextes empreints d'incertitude, d'imprévisibilité et d'instabilité lorsque le rythme des changements s'accélère. La planification à l'aide de scénarios peut également constituer un précieux complément au processus de gestion des risques d'une organisation, afin d'évaluer l'efficacité des stratégies, des tactiques et des plans en fonction de divers environnements futurs possibles.

6.3 Évaluer le programme de gestion des risques

Après que le programme de gestion des risques a été mis en place et qu'un délai approprié s'est écoulé (généralement, de neuf mois à deux ans), le conseil d'administration et/ou la haute direction doivent vérifier si le programme fonctionne comme prévu. Voici certaines des étapes à suivre :

- Obtenir une rétroaction qualitative fournissant des indications quant à la question de savoir si le programme de gestion des risques génère de la valeur pour le conseil d'administration, la haute direction et les autres parties prenantes. Les questions à se poser comprennent les suivantes :
  - Les membres du conseil d'administration sont-ils suffisamment mobilisés, et posent-ils des questions approfondies sur le risque?
  - Le conseil d'administration et/ou la haute direction exercent-ils activement leur fonction de surveillance des risques conformément à la politique de risque?
  - La planification stratégique tient-elle compte du fait qu'il faut identifier et évaluer les risques, et y répondre?
  - Sur quels renseignements peut-on s'appuyer pour évaluer le résultat quantitatif/financier du programme de gestion des risques?
    - Y a-t-il moins de surprises qu'au cours des années précédentes?
    - Les résultats nets sont-ils plus prévisibles?
    - La performance de l'organisation s'est-elle améliorée?

21 Lignes directrices sur la comptabilité de gestion, *Planification à l'aide de scénarios*.

- Examiner les pratiques et les composantes de gestion des risques (par exemple, propension au risque, indicateurs clés de risque) par rapport à la performance stratégique et opérationnelle continue de l'organisation, en particulier à l'égard d'événements spécifiques susceptibles de s'être produits. Des changements doivent alors être apportés, au besoin.
- Comparer le programme de gestion des risques à celui de types similaires d'organisations et d'industries, afin de cerner les éléments à améliorer. Explorer les occasions de communiquer avec des acteurs du domaine de la gestion des risques ne faisant pas partie de l'organisation, afin d'enrichir cette comparaison.

Principaux constats

Sommaire

Toutes les organisations connaissent des événements négatifs, qu'ils soient d'origine externe ou interne. Toutefois, il est fort probable que les organisations dotées de programmes de gestion des risques identifieront ces événements plus rapidement et qu'elles en réduiront au minimum les incidences ou les géreront de manière plus efficace.

Les organisations de toute taille tireront parti de la mise en œuvre d'un programme de gestion des risques. La gestion du risque en entreprise peut aider les organisations à accroître leur valeur, à atteindre leurs objectifs et à répondre à bon nombre des exigences réglementaires ou des parties prenantes, notamment l'adoption de pratiques exemplaires en matière de gouvernance, de risque et de conformité. Les étapes et les pratiques de gestion des risques décrites dans les présentes lignes directrices visent à aider les organisations à faire preuve de résilience face aux risques.

Les conseils et les outils présentés dans ce cadre en six étapes devraient permettre à une organisation de petite ou de moyenne taille de mettre en œuvre un programme de gestion des risques qui appuie les objectifs stratégiques et opérationnels dans un environnement en constante évolution et souvent marqué par des perturbations.

Ressources

Références

- Accountancy Europe. *SME Risk Management. How can your accountant help?*, [En ligne], février 2020.
- Chapelle, Ariane. *Operational Risk Management - Best Practices in the Financial Services Industry*, Wiley and Sons, 2019, p. 37.
- Chapelle, Ariane. *Reflections on Operational Risk Management*, Risk Books, 2017.
- COSO. *Enterprise Risk Management – Integrating with Strategy and Performance*, 2017.
- Rittenberg et Martens. *Enterprise Risk Management - Understanding and Communicating Risk Appetite*, COSO, Thought Leadership Series, 2012.
- CPA Australia. *Risk Management Guide for Small to Medium Businesses*, 2009.
- Dionne, Georges. *Risk Management: History, Definition, and Critique*, [En ligne], Social Science Research Network (SSRN), 2013. [Wiley Online Library]
- Institute of Operational Risk. *Key Risk Indicators*, [En ligne], novembre 2010.
- Marks, Norman. *Governance, Risk Management and Audit*, [En ligne], mars 2018.
- Northbridge Assurance. *Détecter les risques cachés liés à la fabrication*, [En ligne], juillet 2017.
- Organisation internationale de normalisation (ISO). ISO 31000, Management du risque – Lignes directrices, [En ligne], 2018.
- Société ontarienne d'assurance-dépôts. *Cadre de la gestion du risque d'entreprise et Guide d'application : Gestion du risque d'entreprise*, [En ligne], janvier 2018.
- Stanton, Thomas H. *Enterprise Risk Management*, [Vidéo en ligne], conférence TED, mars 2017.
- Table ronde « Leading Practices in Implementing Risk Management », présidée par Stephen Mallory, [En ligne], FEI Canada, 2015.

Ressources de CPA Canada citées

- *20 Questions que les administrateurs d'organismes sans but lucratif devraient poser sur les risques* (2009).
- *Un cadre de surveillance des risques à l'intention des conseils d'administration* (2020).
- *Une gestion intégrée plutôt qu'autonome : Intégrer la gestion des risques à la gestion de l'organisation* (2015).
- Lignes directrices sur la comptabilité de gestion, *Planification à l'aide de scénarios* (2018).
- *L'état de la GRE au Canada : enquête d'étalonnage* (2018).

Ressources supplémentaires de CPA Canada

- *Inducteurs de changement : Prendre l'avenir en main* (2017).
- *Élaboration d'une stratégie efficace pour parer à l'incertitude*, Parties I et II (2015).

Lignes directrices sur la comptabilité de gestion de CPA Canada :

- *Engaging Change – Using a Learning Approach to put the Humanity back into Change Management* (2020) (traduction à venir).
- *Gestion du changement organisationnel – Le modèle de parcours du changement pour favoriser la durabilité organisationnelle* (2020).
- *La courbe risque-valeur du CAM-I : Comprendre votre propension au risque en vue de créer de la valeur* (2020).
- *RÉSILIENCE + ADAPTABILITÉ + INNOVATION = Durabilité. Le cadre RAID, reflet d'une nouvelle mentalité* (2020).
- *L'état actuel de la gestion des risques d'entreprise au Canada* (2016).

Other resources

- Forum économique mondial. *Rapport sur les risques mondiaux de 2020* (2020).
- IFAC. *Optimiser l'apport des comptables à la gestion des risques d'entreprise* (2019).

À propos des auteurs

Bill Wesioly est conseiller en gestion des risques et coach en leadership. Son but est d'améliorer l'efficacité des personnes et des organisations.

Il a acquis de l'expérience dans le secteur des services financiers, d'abord chez BMO, puis chez RBC. Il a passé les 15 dernières années de sa carrière bancaire dans le domaine de la gestion des risques, où il a réussi à élaborer et à diriger des programmes concernant l'évaluation des risques et des contrôles, les scénarios des risques opérationnels et les indicateurs
clés de risque.

M. Wesioly donne actuellement divers cours en gestion des risques pour CPA Ontario, CPA British Columbia, CPA Alberta, CPA Nouveau-Brunswick, CPA Nova Scotia et CPA Newfoundland and Labrador. Il enseigne aussi au Centre of Outsourcing Research and Education (CORE) et a récemment agi comme consultant en gestion des risques auprès de coopératives de crédit, d'écoles privées indépendantes et des Premières nations.

Guenther Moeller est consultant en gestion des risques. Il s'emploie surtout à soutenir les organisations qui mettent en œuvre des pratiques de gestion des risques simples et utiles qui les aident à atteindre leurs objectifs opérationnels.

Il a acquis de l'expérience dans le secteur des services financiers, d'abord auprès de BMO Nesbitt Burns, puis de BMO Services d'entreprise et enfin de TMX. Sa carrière en gestion des risques s'étend sur 20 ans et a été axée sur l'élaboration de pratiques de gestion des risques efficaces et à valeur ajoutée avec les organisations ainsi que sur l'amélioration de leurs capacités en matière de gestion des risques, des notions qu'il a enseignées après avoir élaboré des modules de formation en gestion des risques.

AVERTISSEMENT

La présente publication, préparée par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité.

CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de cette publication.