CHAIRE d'information financière et organisationnelle
ESG UQÀM

Cahier de recherche 2015-04

Les meilleures pratiques en matière de gestion des risques opérationnels : une approche actuelle.

Jaime Leonardo Henriques
Audit, Risk manager, Prudential Brésil

Hanen Khemakhem Ph.D.
Université du Québec (Montréal), École des sciences de la gestion, 315 est Ste-Catherine, R-4570, Montréal, Québec; Chaire d'information financière et organisationnelle, ESG-UQAM.

Juin 2015

Les meilleures pratiques en matière de gestion des risques opérationnels : une approche actuelle

1. Introduction

Traités auparavant comme des risques résiduels, les risques opérationnels sont devenus une catégorie de risque propre et règlementée d'abord par le secteur bancaire (Formule de Bâle II, 2004) et, ensuite, par le secteur européen d'assurance (Solvabilité II, 2009).

Le COSO II, lancé en 2004, a procuré aux sociétés un modèle de gestion intégrée des risques plus robuste, y compris le risque opérationnel, ce qui protège et améliore la valeur de l'entreprise en permettant l'identification, l'évaluation et la gestion des risques selon le niveau de risque qu'elle est prête à accepter.
D'abord, on met en lumière les définitions de risque et de gestion des risques et l'importance de la définition de l'appétence au risque, ainsi que les approches et les techniques les plus utilisés en matière de gestion des risques, de risques opérationnels et de mappage de risques.
Selon le grand dictionnaire terminologique (GDT) de l'office québécois de la langue française, l'exposition à un risque est définie comme « le fait d'être en situation d'assumer ou de subir un risque »[1].Quant à lui, COSO[2] (2004) a défini le risque comme un évènement qui empêche ou mine la création de valeur d'une entreprise.

Dans le monde des affaires, l'interprétation du risque ne repose pas seulement sur cette vision strictement négative. Selon le standard ISO[3] 31000 (2009), « le risque, c'est la conséquence de la définition et de la poursuite des objectifs ciblés par la société dans un environnement incertain.» Encore selon ce standard, le

[1] Article tiré du *Dictionnaire de la comptabilité et de la gestion financière*, version 1.2, reproduit sous licence.
[2] COSO – *"Committee of Sponsoring Organizations of the Treadway Commission"*
[3] ISO – *"International Organization for Standardization"*

risque n'est ni positif ni négatif; il s'agit tout simplement des conséquences des expériences d'une société, ceux qui peuvent apporter des pertes ou des gains.

Cette définition est corroborée par Naciri (2011). Selon cet auteur, les évènements qui se produisent dans une société peuvent influencer son résultat positivement ou négativement. Donc, le risque d'affaires est associé à l'incertitude qui caractérise les résultats de la société selon son secteur d'activité.

Des facteurs internes et externes de risque peuvent générer des résultats négatifs à une entreprise, comme la situation économique ou des faiblesses opérationnelles. Aussi, des résultats positifs peuvent ressortir lors de l'identification et de la mise en pratique d'opportunités reliées aux objectifs, à la stratégie et à l'appétence au risque de l'entreprise.

Donc, afin de préserver leur pérennité, les entreprises doivent être en mesure de mitiger leurs expositions aux facteurs internes et externes de risque les affectant négativement, ainsi que profiter des opportunités de création de valeur pour atteindre ou dépasser leurs objectifs.
La gestion des risques vise justement à mitiger ces expositions aux facteurs de risque. Selon Naciri (2011), la capacité de traiter le risque en termes quantifiables est une des forces de la gestion moderne.

2. L'appétence au risque et l'établissement d'une politique de gestion des risques

Selon Knight et Pretty (2000), afin d'évaluer des risques et de prendre des décisions de la meilleure façon possible, il faut que des sociétés déterminent leur appétence au risque pour des fins de protection ainsi que pour qu'ils créent de la valeur. Cette appétence définit la tolérance au risque que l'entreprise est prête à accepter, ainsi que les dispositions avec lesquelles ils seront traités. Encore selon ces chercheurs, la tolérance aux risques guidera les gestionnaires lors de l'établissement de la stratégie et des objectifs de l'entreprise, où des traitements d'évitement, de réduction, de partage ou d'acceptation des risques seront mis en pratique afin d'assurer les résultats attendus.

L'appétence au risque entrainera une politique du risque où, selon Knight et Pretty (2000), le facteur clé sera l'assurabilité des valeurs tangibles et intangibles de l'entreprise. Cette politique définira les risques comme assurables (transfert au marché et capacité de se prémunir à court terme) et non assurables (gestion

stratégique). Cette politique traite d'un certain nombre d'aspects et définit les paramètres de mise en œuvre qui seront appelés «principes directeurs».

Le COSO a lancé en 2012 un document appelé « Understanding and Communicating Risk Appetite » où il définit l'appétence au risque comme le montant de risque, à un niveau général, qu'une société est prête à accepter lors de la poursuite de création de valeur. Ce document sert à aider les sociétés à créer et à communiquer de façon claire leur appétence au risque, ce qui les aidera à déterminer et poursuivre leurs objectives selon les risques qu'elles sont prêtes à accepter.

3. La gestion des risques

3.1 Définition et historique

Selon le Secrétariat du Conseil du Trésor du Canada (2010), la gestion du risque est « une démarche systématique visant à établir la meilleure façon de procéder dans des circonstances incertaines par la détermination, l'évaluation, la compréhension, le règlement et la communication des questions liées aux risques.» Cet organisme a aussi définit la gestion intégrée des risques comme : « une démarche systématique, continue et proactive visant à comprendre, à gérer et à communiquer les risques du point de vue de l'ensemble de l'organisation. Elle favorise la prise de décisions stratégiques qui contribuent à l'atteinte des objectifs globaux de l'organisation ».

Le standard ISO 31000 (2009) définit la gestion de risques comme « un processus d'optimisation qui fait l'accomplissement des objectifs plus probable ».

L'ISO est l'acronyme abrégé de « organisation mondial de normalisation ». C'est le premier producteur de normes internationales d'application volontaire dans le monde. Élaborées dans le cadre d'un consensus mondial, elles aident à supprimer les obstacles au commerce international. En 2009, cet organisme a publié l'ISO 31000-2009, une norme globale sur la gestion des risques, avec le but de fournir une façon plus simple de penser les risques et leur gestion, tout en réglant les incohérences et les diverses ambiguïtés existant aujourd'hui à cause des différentes approches et définitions (Purdy, 2010).

Le COSO 2 (2004) définit la gestion intégrée des risques comme « le processus appliqué dans la stratégie et à travers les activités de la société relevant du conseil d'administration, des dirigeants, des cadres et du personnel de la société. Ce processus vise à identifier les événements potentiels qui peuvent affecter la société et gérer les risques selon sa tolérance pour fournir une assurance raisonnable quant à la réalisation des objectifs corporatifs.»

Le COSO est l'acronyme de « *Committee of Sponsoring Organizations* ». C'est une organisation sans but lucratif du secteur privé qui sert à guider les entreprises vers une gestion d'affaires efficiente, efficace et éthique. Au début des années 90, le COSO a diffusé le système d'évaluation des contrôles internes (COSO 1), ce qui est devenu le référentiel des entreprises suite à la promulgation de la loi SOX[4] aux États-Unis. Ce référentiel traite le contrôle interne comme un moyen de certifier l'efficience et l'efficacité des opérations, la fiabilité des informations financières et la conformité de l'entreprise aux règlements et lois existants.

L'an 2001 marque le départ du nouveau projet de la commission : le COSO 2. Ce nouveau projet visait le développement d'un outil de gestion intégrée des risques plus robuste qui permettait aux entreprises l'identification, l'évaluation et la gestion de leurs risques selon leur niveau de tolérance.

En 2004, le COSO (Committee of Sponsoring Organizations) a lancé un cadre modèle de la gestion intégrée des risques, ce que l'on appelle COSO 2. Selon le COSO (2004), il ne remplace pas le système des contrôles internes. En fait, il l'incorpore afin de donner les résultats les plus solides possible. Ce modèle est un outil de gestion intégrée des risques plus robuste qui protège et améliore la valeur de l'entreprise en permettant l'identification, l'évaluation et la gestion des risques selon le niveau de risque qu'elle est prête à accepter (tolérance au risque).

Le modèle de gestion intégrée des risques des entreprises (COSO 2, 2004) repose sur huit éléments inter reliés directement attachés aux objectifs de la société: l'environnement interne, la fixation des objectifs, l'identification des événements, l'évaluation des risques, le traitement des risques, les activités de contrôle, l'information et communication et le pilotage. Ces huit éléments constituent un critère d'efficacité de la gestion des risques au moment où ils sont mis en pratique efficacement par la gestion de la société.

[4] Sarbanes-Oxley Act, 2002.

3.2 Les intervenants dans le processus de la gestion des risques

Selon le COSO 2 (2004), la gestion intégrée des risques est « *le processus appliqué dans la stratégie et à travers les activités de la société relevant du conseil d'administration, des dirigeants, des cadres et du personnel de la société ».*

- **Rôle du conseil d'administration**

La séparation entre la propriété et le contrôle entraine une division de la structure décisionnelle d'une entreprise en deux parties majeures : d'une part, la gestion de la décision, où les dirigeants jouent les rôles d'initiative et d'implémentation; et, d'autre part, le contrôle de la décision, où les propriétaires, à travers le conseil d'administration, jouent les rôles d'approbation et de surveillance (Fama et Jensen, 1983). Cette structure de séparation du processus de décision sert à réduire les pouvoirs des dirigeants et il se fait plus nécessaire dans les entreprises où la prise de décision dépend d'informations qui viennent de plusieurs dirigeants.

Naciri (2011) propose un concept de gouvernance qui dépasse le but ultime de protéger et maximiser la richesse des actionnaires. Sa pensée repose sur le concept de gouvernance comme l'utilisation efficace et conforme à l'éthique des ressources organisationnelles.

Encore selon Naciri (2011), parmi d'autres responsabilités, relève aussi du conseil d'administration la surveillance de l'efficacité des systèmes d'information, des contrôles internes et de la gestion des risques. Donc, afin de faire face aux responsabilités mentionnées ci-dessus, le conseil d'administration constitue un comité d'audit dans l'objectif de chapeauter la direction et de s'assurer que celle-ci effectue une gestion compétente et éthique de l'entreprise.

Knechel et Willekens (2006) ont analysé la relation entre la gestion des risques et la surveillance du conseil d'administration et les demandes de service d'audit externe. Ils ont trouvé une réduction du coût

du service d'audit lorsqu'une entreprise présente une gestion de risques conforme aux règlementations de haut niveau.

- **Le dirigeant et la gestion des risques**

Selon Archer (2002), le premier pas vers la création d'un système de gestion des risques est le choix du professionnel qui fera cette gestion et qui donnera du soutien au Président de la société, aux dirigeants et au conseil d'administration, ainsi qu'au comité d'évaluation des risques composé de représentants de plusieurs secteurs de l'entreprise, y compris l'audit interne.

Donc, le principal rôle de ce processus est développé par le professionnel qui ira mettre en œuvre la gestion des risques. C'est à lui que revient la tâche de délimiter les responsabilités selon chaque risque, de coordonner les décisions liées aux risques, d'établir la liste des priorités et de les communiquer au directeur général (Knight et Pretty, 2000).

- **Les dirigeants et le personnel de la société**

Le processus de gestion des risques doit être amorcé au sommet de la hiérarchie organisationnelle. « Il relève de la direction de créer une culture organisationnelle saine, sensibiliser au risque, garantir l'efficacité ainsi que la mise en application des stratégies adoptées par l'entreprise. En plus, la direction doit fournir l'assurance que le personnel est engagé concernant la gestion quotidienne de ces risques» Naciri (2011).

La vision du COSO (2004) se présente similaire à la vision de Naciri (2011). Le président de la société apparaît comme l'acteur principal de la gestion des risques. Ce sont lui et les autres dirigeants qui vont appuyer la philosophie du risque établie par le conseil d'administration de la société en la gérant selon son appétence au risque. Les autres membres de la société sont responsables de la mise en application de la gestion des risques en respectant les directives et les protocoles adoptés par la société.

Le risque opérationnel est définit comme la possibilité d'occurrence de pertes découlant de fautes, de faiblesses ou de l'inadéquation de processus internes, de personnes et de systèmes, ou découlant de fraudes ou des évènements externes, en incluant le risque juridique et en excluant les risques liés aux décisions stratégiques et à la réputation de la société (SUSEP, 2013).

4. Les méthodes de gestion des risques

Le COSO (2004) présente deux types de risques : inhérents et résiduels. Les risques inhérents sont ceux qui existent avant les traitements des risques, tandis que les risques résiduels sont ceux qui persistent même après la mise en œuvre des traitements des risques.

Selon le COSO (2012), il y a certaines entreprises qui assument les risques inhérents comme ceux reliés à l'inefficacité des traitements de risque et les risques résiduels comme ceux attendus après le déploiement et le bon fonctionnement de ces traitements de risque.

Deux principales méthodes sont utilisées lors de la mise en œuvre d'un modèle de gestion des risques : la traditionnelle et l'intégrée.

4.1 L'approche traditionnelle de gestion des risques

Comme Liebenberg et Hoyt (2003) ont bien expliqué : l'approche traditionnelle de gestion des risques se caractérise par la gestion séparée des catégories de risque. Selon cette approche, on traite les risques opérationnels, de marché, de crédit et de liquidité par des silos. À l'opposé, encore selon ces derniers, la gestion intégrée des risques considère chaque catégorie comme une partie du risque globale de l'organisation, permettant que les sociétés puissent évaluer les interactions entre les risques et identifier l'impact potentiel qu'ils peuvent y apporter.

Selon le guide appelé « Risk Assessment in Practice », lancé par COSO en 2012, l'ensemble de risques ne correspond pas à la somme des parties (silos). Pour comprendre le portefeuille de risques, il faut comprendre les risques des éléments individuels et leurs interactions dues à la présence de couvertures naturelles et d'amplification mutuelle de risques. Pour ce faire, il faut décomposer les silos.

4.2 La gestion intégrée des risques

Selon Liebenberg et Hoyt (2003), un signal de l'existence de la gestion intégrée des risques est la présence d'un gestionnaire de risques, engagé pour mettre en place et gérer ce système.

Encore selon ces chercheurs, les sociétés les plus efficaces sont plus assujetties à l'adoption d'un système de gestion des risques en fonction de sa capacité de réduire les coûts associés aux problèmes de changement de la caractéristique du risque et de communiquer le profil de risques de la société aux parties prenantes externes.

Au regard de Colquitt, Hoyt, et Lee (1999), le niveau de la gestion intégrée des risques s'explique en fonction de la taille et du secteur de la société ainsi qu'en fonction de l'expertise du professionnel engagé pour gérer les risques. Beasley et al. (2005) ont remarqué que, malgré le moment de croissance de l'adoption de la gestion des risques en tant que mécanisme interne de gouvernance, ce ne sont pas toutes les organisations qui adoptent la gestion intégrée des risques. Ils ont démontré que la présence d'un gestionnaire de risques a une association positive avec le stade de développement du système de gestion intégrée des risques au sein de l'entreprise.

Le COSO a lancé en 2012 le guide appelé « *Risk Assessment in Practice* » procurant un aperçu des approches et techniques les plus utilisées en matière d'évaluation des risques. Celui-ci sert à aider les sociétés à poursuivre la maturation de leurs systèmes de gestion intégrée des risques.

Outre les critères de fréquence et d'impact, ce guide présente deux autres variables considérées actuellement par plusieurs sociétés : la vulnérabilité de la société au risque et la vitesse à laquelle il peut émerger. Ces deux derniers critères permettent à société de connaître les effets d'un risque en ce qui concerne sa vitesse d'apparition, ainsi que le temps d'arrêt tolérable d'une activité considérée à risque et la vitesse de mitigation de ce risque.

Scandizzo (2005) propose une méthodologie de registre des risques opérationnels servant à identifier les risques inhérents présents à chaque étape des processus d'affaires à travers l'étude des conducteurs et des facteurs de risque. Selon lui, le registre des risques peut être défini comme un outil capable d'extraire des informations spécifiques concernant les faiblesses existantes à chaque processus de la société.

Généralement, l'évaluation des facteurs de risque pouvant entraîner des résultats négatifs pour une société est enregistré dans une matrice des risques.

5. La matrice des risques

Selon le Secrétariat du Conseil du Trésor du Canada[5], la matrice des risques « est un outil servant à illustrer le classement des risques en fonction de l'évaluation de leur probabilité et de leur incidence ».

Parmi les divers outils d'évaluation des risques, la matrice des risques se démarque grâce à sa simplicité de gestion ainsi qu'à son grand pouvoir de communication visuelle.

Sous la forme d'un graphique, la matrice des risques, avec ses deux axes principaux (soit probabilité et impact), sert à évaluer les facteurs de risques. L'espace graphique est généralement divisé en trois champs de risques : bas, moyen et haut. Ces champs sont représentés par des couleurs, généralement le vert pour les risques faibles, le jaune pour les risques moyens et le rouge pour les risques élevés.

Les critères sont évalués à l'aide d'une échelle de ratios de risque. Selon le COSO (2012), l'échelle la plus pratiquée actuellement est celle de 5 niveaux, car elle procure une précision plus élevée en ce qui concerne l'analyse qualitative. La même étude (COSO, 2012) propose aussi une flexibilité, en ce qui concerne l'échelle de ratio de risque, en fonction du secteur, de la grandeur, de la complexité et de la culture des sociétés.

Cox (2008) souligne le manque d'articles scientifiques qui abordent la performance des matrices de risques sur les décisions reliées à la gestion de risques. De plus, il signale l'insuffisance de littérature technique démontrant les limites logiques et mathématiques des matrices des risques.
En analysant les propriétés mathématiques des matrices de risques, l'auteur a trouvé plusieurs limites de cet outil de gestion de risque, comme le côté subjectif de l'interprétation de la fréquence et les

[5] Secrétariat du conseil du trésor du Canada http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/gcrp-gepro03-fra.asp

conséquences lors de l'évaluation d'un risque. Ces limitations rendent extrêmement nécessaire la présentation d'explications sur un classement lors d'une prise de décision basée sur la matrice de risques.

6. Les risques opérationnels

La formule de Bâle II (2004) présente la définition universelle de risque opérationnel, comme suit : « Le risque opérationnel se définit comme le risque de pertes résultant de carences ou de défauts attribuables à des procédures, personnels et systèmes internes ou à des évènements extérieurs». La définition inclut le risque juridique, mais exclut les risques stratégiques et de réputation.

En convergeant avec la formule de Bâle II, la Surintendance des assurances privées (SUSEP, 2013) définit le risque opérationnel comme « la possibilité d'occurrence de pertes découlant de fautes, de faiblesses ou de l'inadéquation de processus internes, de personnes et de systèmes, ou découlant de fraudes ou des évènements externes, en incluant le risque juridique et en excluant les risques liés aux décisions stratégiques et à la réputation de la société ».

Les risques opérationnels se différencient des autres parce que ce sont des risques inhérents au déroulement naturel de l'activité ou des activités de la société. Leur mauvaise gestion peut entraîner la présentation d'un profil de risque incohérent qui expose la société à des pertes (comité de Bâle sur le contrôle bancaire, 2003).

La catégorie opérationnelle est basée sur l'efficacité et l'efficience des ressources investies dans l'entreprise. Selon Pezier (2002), les entreprises présentant des fonctions et des responsabilités assez fragmentées sans échange cognitif adéquat et sans lignes directrices bien présentées ou celles qui permettent l'existence de comportements douteux en matière d'éthique et des abus d'autorité sont fortement exposées à des problèmes opérationnels.

Le référentiel COSO II (2004)[6] divise les objectifs d'une organisation en quatre catégories qui peuvent être entravés par les risques: stratégiques, opérationnels, de divulgation et de conformité. Parmi ces catégories, cette étude se penchera sur celle déterminant la performance de l'entreprise, autrement dit, la catégorie des objectifs opérationnels.

[6] COSO – "*Committee of Sponsoring Organizations of the Treadway Commission*"

6.1 La démarche d'identification et d'évaluation des risques opérationnels

Dans ce qui suit, on présente les référentiels généralement utilisés en gestion des risques afin d'identifier et d'évaluer des risques opérationnels. L'article à Scandizzo (2005) propose l'identification des risques inhérents présents à chaque étape des processus d'affaires à travers l'étude des conducteurs et des facteurs de risque, **t**andis que le COSO (2012) présente les meilleures pratiques en matière d'analyse de ces risques.

6.1.1 Le modèle de Scandizzo (2005) pour l'identification des risques opérationnels

Scandizzo (2005) propose une méthodologie de mappage des risques opérationnels identifiant les risques inhérents présents à chaque étape des processus d'affaires à travers l'étude des conducteurs et des facteurs de risque. Son explication se retrouve à l'étape 2 de la méthodologie, proposée par l'auteur, mise en lumière dans cette section. De plus, celui-ci présente le tableau de bord des risques opérationnels; ce qui nous permet d'identifier le profil de risque opérationnel de la société.

La méthodologie proposée par cet auteur repose sur 5 étapes, comme suit :

1. L'identification des activités majeures en deux niveaux: D'abord, identification et documentation des activités avec un regard plus large. Après, ramassage d'informations plus détaillées afin d'identifier des faiblesses existantes des processus.

2. L'identification de failles opérationnelles aux activités à partir des conducteurs et des facteurs de risque. Les composants des conducteurs de risques sont : des personnes, des processus, de la technologie et des facteurs externes.

3. Pour évaluer ces composants, les gestionnaires doivent prendre en compte les facteurs de risques. Ces facteurs servent à démontrer les failles qui peuvent émerger en cas de faible performance des conducteurs de risques. Les facteurs de risques les plus utilisés lors de l'évaluation des conducteurs sont : la qualité, la quantité, la disponibilité et la rupture des conducteurs de risques. Identification et documentation, par des processus, de tous les risques inhérents reliés aux activités de la société.

4. Identification et analyse des pertes. C'est l'étape clé, puisqu'il représente le moment où la priorisation et le traitement des risques sont réalisés.

5. Choix des indicateurs de risques clés servant à identifier en avance qu'un risque peut se concrétiser et affecter négativement la valeur de la société, ainsi que le déploiement de contrôles internes capables de mitiger les risques auxquels la société est exposée.

La méthode d'identification des risques de l'étude proposée repose sur les trois premières étapes de l'ouvrage de Scandizzo (2005). L'auteur propose une méthodologie de mappage des risques qui identifie les risques inhérents présents à chaque étape des processus d'affaires à travers l'étude des conducteurs et des facteurs de risque. De plus, il présente le tableau de bord des risques opérationnels, ce qui nous permet d'identifier le profil de risque opérationnel de la société. L'adoption des trois premières étapes de l'ouvrage de Scandizzo (2005) servira de guide de bonnes pratiques en matière d'identification des risques et nous permettra de savoir comment les gestionnaires de la société envisagent le modèle idéal d'identification des risques.

6.1.2 L'évaluation des risques opérationnels dans la pratique (COSO, 2012)

La valeur de la société est maximisée lorsque sa gestion aligne sa stratégie et ses objectifs pour atteindre un équilibre optimal entre la croissance et les résultats attendus et les risques potentiels à accepter (COSO, 2004).

La présente étude se penchera sur la catégorie d'objectifs opérationnels. Cette catégorie de risque est un facteur déterminant pour la performance de la société (COSO 2004).
Le COSO a lancé en 2012 un guide appelé « Risk Assessment in Practice ». Il comprend les risques opérationnels et procure un aperçu des techniques les plus utilisées lors du processus de prise de décision. Basé sur l'élément d'évaluation des risques, ce guide apporte de nouveautés au niveau des critères d'évaluation des risques et sert à aider les sociétés à poursuivre la maturité de leurs systèmes de gestion des risques.

Outre les critères de fréquence et d'impact, ce guide présente deux autres variables considérées actuellement par plusieurs sociétés : la vulnérabilité de la société au risque opérationnel et la vitesse qu'il peut émerger. Ces deux critères permettent à société de connaître les effets d'un risque en ce qui concerne sa vitesse d'apparition, ainsi que le temps d'arrêt tolérable d'une activité par la société et la vitesse de mitigation de ce risque.

Le critère d'évaluation de la vulnérabilité de la société repose sur sa capacité de prévoir, à travers les tests d'efficacité des réponses aux risques (y compris les contrôles internes), des scénarios de failles des traitements donnés aux risques, préparant des plans d'action qui puissent remédier ces situations en temps opportun. De plus, ce critère repose sur sa capacité de résister financièrement à ces événements de façon solide.

Le critère d'évaluation de la vitesse d'apparition d'un événement repose sur la capacité de prévoir le temps d'action que la société dispose entre l'apparition de cet événement et ses premiers symptômes.

Les sociétés ont reconnu au cours des années l'importance d'évaluer les interactions entre les risques à cause de l'impact potentiel qu'ils peuvent y apporter. Ce guide met en lumière les techniques d'évaluation des risques à conséquences multiples les plus appliquées telles que les matrices d'interaction des risques, les diagrammes « *bow-tie* » et distributions de probabilités agrégées.

La gestion des risques opérationnels repose sur deux étapes et deux types de traitements : le qualitatif et le quantifiable. Le traitement qualitatif correspond à la première étape, ce qui consiste à évaluer et à classer de façon descriptive chaque risque opérationnel identifié par la société. La deuxième étape sert à mesurer les risques opérationnels les plus importants à travers les traitements quantitatifs, malgré l'existence de risques non mesurables.

Les techniques d'évaluation qualitative des risques opérationnels les plus utilisées sont les entrevues, les ateliers, les sondages, les analyses comparatives et les analyses de scénarios, tandis que les techniques quantitatives font l'utilisation d'analyses comparatives et d'analyses de scénarios pour générer des estimations ponctuelles prospectives et des distributions prévisionnelles.

Donc, la société identifie ses risques opérationnels et les évalue en appliquant des techniques qualitatives d'évaluation dans une première étape. Ensuite, les risques les plus élevés sont évalués au niveau des interactions existantes entre eux, ce qui produit de nouveaux résultats concernant leurs évaluations. Finalement, ces risques sont listés dans une matrice de risques par ordre décroissante d'importance, ce qui permet la priorisation et, conséquemment, le report des risques les plus importants aux gestionnaires et au conseil d'administration.

Le guide renforce aussi l'échange cognitif entre ceux qui sont plus proches des risques et la gestion de la société. Cet échange permet le traitement des risques de façon plus consistante et complète. De plus, ce comité détache l'importance de l'automatisation du système de gestion des risques, y compris le risque opérationnel, comme facteur clé d'efficience, indispensable au fur et à mesure que la complexité, le dynamisme et la distribution géographique de la société deviennent plus élevées. Les approches et techniques soulevées par le guide du COSO comme les plus utilisées lors du processus d'évaluation des risques opérationnels seront considérées dans cette étude comme des procédures standards. Cela permet de fournir aux gestionnaires, y compris les contrôleurs internes, un modèle à suivre en matière d'évaluation de ces risques.

7. La réglementation du risque opérationnel

Les conseils d'administration sont de plus en plus invités à surveiller de façon plus efficace le système de gestion des risques des sociétés. Cela est principalement dû à la croissante préoccupation de réglementation de la gestion des risques (COSO, 2010).
En 2004, la Bourse de NY a imposé aux sociétés listées un règlement7 qui implique les comités d'audit dans la surveillance du système de gestion des risques mis en pratique par des gestionnaires. En 2008, l'agence de notation Standard & Poor's a commencé à évaluer la gestion intégrée des risques en tant qu'élément d'analyse de risque de crédit. En 2009, la « Securities and Exchange Commission (SEC) » a imposé aux sociétés la divulgation du niveau d'engagement des administrateurs par rapport à la surveillance de la gestion des risques. L'année 2010 est marquée par la réforme financière fédérale américaine.

[7] *NYSE, Règles sur gouvernance corporative – Section 303-A*

Traités avant comme des risques résiduels, les risques opérationnels sont devenus une catégorie de risque propre et réglementée en 2004, lors de la divulgation de la formule de Bâle II par le comité de Bâle sur le contrôle bancaire.

Cette formule règlemente la création de fonds propres capables de faire face aux risques acceptés par les banques, y compris les risques opérationnels, étant la gestion de ces risques supervisée par la réglementation du secteur bancaire. De plus, la formule de Bâle établit le besoin de transparence lors de la divulgation des informations au marché. Membre effectif du comité de Bâle, la Banque Centrale du Brésil a établi le chronogramme final de mise en œuvre de la formule de Bâle en 2009.

En 2009, le Conseil et le Parlement européen ont adopté le projet qui s'appelle Solvabilité II. Selon la fédération française des sociétés d'assurances, il s'agit d'une « réforme des règles européennes garantissant la solvabilité des sociétés d'assurances. La réforme a pour ambition d'adapter le niveau des capitaux propres aux risques réels auxquels elles sont exposées ». Basée sur la formule de Bâle II, la Solvabilité II définit les risques opérationnels en tant que catégorie propre et règlementée. Cette réforme détermine la création de fonds propres capables de faire face aux risques, y compris les risques opérationnels, acceptés par les sociétés d'assurance-vie, étant la gestion de ces risques supervisée par les agences de réglementation du secteur.

L'étude développée par KPMG8 en 2011 sur la Solvabilité II et la transformation de l'industrie globale d'assurance met en lumière le changement du modèle d'opération de l'industrie d'assurance européenne, dû à l'application de la Solvabilité II, et ses implications en ce qui concerne l'harmonisation de la réglementation de l'industrie d'assurance en échelle globale. Sharara, Hardy et Saunders (2009) ont comparé les exigences américaines, canadiennes et européennes (Solvabilité II) en matière de suffisance de capital pour les sociétés d'assurance-vie. Les résultats ont démontré que les exigences européennes permettent une surveillance plus efficace de la solvabilité des sociétés d'assurance.

8. Conclusion

La crise financière, qui a affecté d'abord les États-Unis en 2008, a eu comme une de ses principales causes les pratiques financières à haut risque. Les prêts hypothécaires à risque ainsi que la titrisation de nouveaux

[8] *KPMG, réseau mondial de prestations de services d'audit, fiscaux et de conseil.*

produits de crédits sophistiqués et complexes non règlementés ont entrainé l'insolvabilité de plusieurs sociétés et la faillite de la géante banque d'investissement "*Lehman Brothers"* le 14 septembre 2008.

Compte tenu du fait que le calcul de la réserve des capitaux propres règlementaires reliée aux risques opérationnels reposera sur les pertes opérationnelles, l'amélioration du système de gestion des risques des sociétés d'assurance a pour effet de diminuer ces pertes et conséquemment la réserve règlementaire de capitaux propres.

L'objectif de ce travail est de comparer les meilleures pratiques en identification et en évaluation de risques ainsi que celles connues et pratiquées par les gestionnaires de la société d'assurance-vie brésilienne. Pour ce faire, nous avons utilisé en tant que point de référence la méthode d'identification des risques opérationnels présentée par Scandizzo (2005) ainsi que les approches et techniques soulevées par le guide du COSO (2012) sur l'évaluation des risques opérationnels.

Il existe un besoin de renforcer la compréhension de la culture des risques parmi les gestionnaires et, à travers eux, parmi les cadres et le personnel de la société. Le rôle du département de gestion des risques d'assister les départements lors de l'identification et de l'évaluation des risques opérationnels, ainsi que la divulgation d'une politique d'appétence aux risques gagnent à être mieux travaillés par la société. La définition de risque inhérent n'est pas claire pour les gestionnaires et cela peut impliquer négativement au moment d'évaluer les risques.

Concernant les méthodes d'identification et d'évaluation de risques, nous suggérons l'harmonisation de ceux pratiquées par les gestionnaires, ainsi que des améliorations qui permettront à la société d'identifier et d´évaluer tous les risques qui l'affectent en faisant l'utilisation de méthodes plus efficaces, comme celles d'identification (Scandizzo, 2005) et d'évaluation (COSO, 2012) des risques opérationnels utilisés dans cet ouvrage comme référence.

Bibliographie :

Archer, D. 2002. « Creating a Risk Management Framework ». CMA Management, vol. 76, nº 1, p. 16 - 20.

Beasley, S., R. Clune et D. R. Hermanson. 2005. « Enterprise Risk Management: An Empirical Analysis of Factors Associated with the Extent of Implementation». Journal of Accounting and Public Policy, vol. 24, p. 521-531.

Colquitt, L., R. E. Hoyt, et R. B. Lee. 1999. « Integrated Risk Management and the Role of the Risk Manager ». Risk Management and Insurance Review, vol. 2, nº 3, p. 43 — 61.

Comité de Bâle sur le contrôle bancaire. 2003. *Saines pratiques pour la gestion et la surveillance du risque opérationnel.* Bâle : Banque des règlements internationaux, 12 pages.

Comité de Bâle sur le contrôle bancaire. 2004. *Convergence internationale de la mesure et des normes de fonds propres (Dispositif révisé)*. Bâle: Banque des règlements internationaux, 216 pages.

Comité de Bâle sur le contrôle bancaire. 2009. Principes fondamentaux en vue de l'établissement de régimes efficaces d'assurance-dépôt. Bâle: Banque des règlements internationaux, 24 pages.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2004. *Enterprise Risk Management—Integrated Framework (Executive Summary).* New York: AICPA, 135 pages.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2012. *Risk Assessment in Practice.* New York: AICPA, 19 pages.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2012. *Understanding and Communicating Risk Appetite.* New York: AICPA, 24 pages.

Cox, L. A.. 2008. « What's Wrong with Risk Matrices? ». Risk Analysis, vol. 28, nº2, p. 497 – 512.

Fama, E. F. et M. C. Jensen. 1983. « Separation of Ownership and Control ». Journal of Law and Economics, vol.26, nº 2, p. 301-325.

Fédération française des sociétés d'Assurances. 3/05/2010. *Webographie - Solvabilité 2 : 10 questions pour comprendre la réforme et ses enjeux.* Récupéré de http://www.ffsa.fr/sites/jcms/p1_81578/solvabilite-2-10-questions-pour-comprendre-la-reforme-et-ses-enjeux?cc=fn_7369

Knechel, W. R. et M. Willekens. 2006. « The Role of Risk Management and Governance in Determining Audit Demand ». Journal of Business, Finance & Accounting, vol. 33, nº 9 et nº10, p. 1344 – 1367.

Knight, R. F. et D. J. Pretty. 2000. « Définir une philosophie du risque». Les Échos – supplément, nº 18299 (13 décembre), pages 6-7.

Liebenberg, A. P. et Robert E. Hoyt. 2003. « The Determinants of Entreprise Risk Management : Evidence from the Appointment of Chief Risk Officers ». Risk Management and Insurance Review, vol. 6, nº 1, p. 37-52.

Naciri, A. 2011. *Traité de gouvernance d'entreprise : l'approche scolaire.* Montréal : Presses de l'Université du Québec, 700 pages.

Organisation internationale de normalisation. 2009. *ISO 31000: 2009 : Management du risque - principes et lignes directrices.* Geneva: Organisation internationale de normalisation, 24 pages.

Organisation internationale de normalisation. 2009. *ISO Guide 73 : 2009 : Management du risque – Vocabulaire.* Geneva: Organisation internationale de normalisation , 15 pages.

Pezier, J. 2002. *Webographie - Operational Risk Management.* Récupéré de http://www.math.ethz.ch/~embrecht/RM/DP2002-21.pdf

Purdy, G. 2010. « ISO 31000:2009—Setting a New Standard for Risk Management». Risk Analysis, vol. 30, nº 6.

Scandizzo, S. 2005. « Risk Mapping and Key Risk Indicators in Operational Risk Management ». Economic Notes by Banca Monte dei Paschi di Siena SpA, vol. 34, nº 2, p. 231–256.

Secrétariat du conseil du trésor du Canada. 11/07/2011. *Guide d'élaboration d'un profil de risque organisationnel.* Disponible à : http://www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/gcrp-gepro03-fra.asp

Secrétariat du Conseil du Trésor du Canada. 19/08/2010. *Cadre stratégique de gestion du risque.* Disponible à : http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=19422&section=text

Sharara, I., M. Hardy, et D. Saunders. 2010. « A Comparative Analysis of U.S., Canadian and Solvency II Capital Adequacy Requirements in Life Insurance ». Society of Actuaries. Working Paper. University of Waterloo.