ALEXANDRA PSICA, CMC
RESPONSABLE DE DIRECTION
INTERIS CONSULTING INC.

Le bon ajustement

Audit des cadres ERM

Les examens d'administration du risque au sein d'une entreprise offrent l'assurance d'une base saine permettant d'évaluer et d'atténuer les risques.

DANS L'ABSOLU, LE CADRE DE MANAGEMENT DES RISQUES DE l'entreprise (ERM) doit être suffisamment adapté à ses objectifs, à ses risques inhérents et à sa tolérance vis-à-vis de ces risques pour lui permettre de tirer parti des opportunités qui se présentent à elle sans pour autant trop l'exposer. Reposant sur la culture du risque propre à chaque organisation, l'ERM centralise l'ensemble des pratiques destinées à évaluer, communiquer et gérer les risques. Un cadre satisfaisant permet à l'organisation de prévoir les conséquences possibles d'événements à venir, d'effectuer les changements nécessaires pour minimiser le risque, de gérer l'issue négative d'un événement et de tirer parti des opportunités de croissance engendrées par ce dernier. Il permet aux responsables d'avoir accès, en temps opportun, à l'information nécessaire à une prise de décision adaptée, dans les plages de tolérance au risque définies, pour atteindre les objectifs de l'organisation. Ce faisant, l'ERM contribue à optimiser l'affectation des ressources et à renforcer la gouvernance. ■ Il favorise également la transparence en donnant l'assurance à la direction, au conseil et aux actionnaires, que les risques sont traités suffisamment tôt pour être maîtrisés. Les risques ne peuvent pas tous être évités, mais une transmission rapide de l'information permet de disposer du temps nécessaire à la prise de décisions appropriées et

d'identifier puis de tirer parti des opportunités potentielles. Les cadres ERM permettent également aux organisations de rapprocher des informations utilisées par différentes fonctions telles que l'audit, la conformité ou le management. ■ Les audits jouent un rôle clé car ils contribuent à assurer que le cadre est à la fois suffisamment bien conçu pour répondre à l'objectif attendu et suffisamment efficace pour apporter de la valeur à l'organisation. Les cadres ERM étant liés aux objectifs, à la taille, à la complexité et à la maturité des organisations, les auditeurs doivent se fier à leur jugement pour conclure sur leur adéquation à leur contexte.

LE RÔLE DE L'AUDIT

Un cadre ERM est un ensemble de pratiques liées à la stratégie d'entreprise reposant sur une culture de l'administration du risque permettant d'évaluer, de gérer et d'informer sur le risque en accord avec les objectifs, les opérations et le profil définis par l'entreprise (voir « Principes directeurs des cadres ERM » page 4). Il est généralement composé de lignes directrices et de procédures simples à utiliser, mais aussi, de processus et de techniques pragmatiques, flexibles en auto-gérance, et enfin d'outils d'administration du risque permettant de l'identifier, de l'évaluer et d'établir des rapports de gestion et un contrôle. Toutefois, d'une entreprise à l'autre ou même au sein d'une même entreprise, le cadre ERM peut considérablement varier en fonction du niveau de risque inhérent associé aux objectifs de l'entreprise et à sa capacité à supporter les risques. Par exemple, le service informatique pourra exiger un cadre avec une identification et une évaluation précises du risque et des procédures graduelles, tandis que les ressources humaines n'exigeront qu'une politique de référence claire et un examen des procédures. Souvent, l'on remarque qu'au sein d'une même entreprise, le service chargé des opérations de transaction est doté d'un cadre ayant fait ses preuves et axé sur la conformité dans lequel les indicateurs de risque sont clairement définis et peuvent même être intégrés aux activités quotidiennes de l'entreprise tandis que le service chargé de la gestion des risques stratégiques aura un cadre moins formel qui nécessite d'être plus développé. Les ressources d'audit interne focalisant majoritairement sur les zones les plus à risque, il est primordial que le cadre ERM fasse l'objet d'un audit régulier de façon à s'assurer de sa capacité à identifier les risques pertinents et ainsi produire des données fiables sur lesquelles seront basées l'attribution des ressources, la planification d'audit et autres décisions. Il est également essentiel de s'assurer de la fiabilité de l'administration du risque dont pourront dépendre plusieurs segments de l'entreprise, et cela, d'autant plus, dans le contexte actuel de recherche de cohésion entre les organisations en termes d'audit, de conformité et d'administration du risque. Les auditeurs doivent tenir compte de tous les objectifs attendus de l'entreprise, du cadre ERM lors de la mise en place de l'audit et du jugement rendu sur l'adéquation du cadre.

La base fondamentale d'un cadre ERM réussi réside dans la capacité de l'auditeur à émettre un jugement pertinent sur l'équilibre optimal entre le niveau de maturité des pratiques ERM et le niveau de risque auquel l'entreprise est confrontée. Au vu de cette pratique d'affaires émergente, on ne peut attendre des entreprises qu'elles exploitent toutes les capacités d'un programme ERM. Il est de la responsabilité de l'auditeur de donner son opinion sur l'objectif de l'audit, ayant trait par exemple à l'efficacité du cadre. Néanmoins, les auditeurs doivent également tenir compte du contexte de l'entreprise, y compris des écarts résultant du délai imparti par l'entreprise pour la mise en

place du cadre et du budget pouvant être réellement attribué au programme ERM. Par ailleurs, les audits doivent prendre en charge la gestion de risque opérationnel (risques occasionnés par les livraisons quotidiennes) et l'administration du risque d'entreprise (risques encourus pour atteindre les objectifs de l'entreprise). L'objectif premier d'un audit de cadre ERM est de contribuer à l'amélioration de la gestion de l'entreprise.

Lors de l'audit d'un cadre ERM, il est important de faire la différence entre l'évaluation de l'efficacité de ce cadre pour l'administration du risque au sein d'une entreprise et la responsabilité de la direction quant à contrôler l'efficacité des décisions d'atténuation du risque individuel. L'audit d'un cadre ERM doit examiner si le cadre lui-même est suffisamment efficace pour aider l'entreprise à gérer les risques et non pas déterminer si la direction a pris des décisions pertinentes en matière de risque. Au sein de nombreuses entreprises, les auditeurs internes optent d'ailleurs pour la sécurité en préservant l'indépendance requise à l'expertise du cadre. En tant qu'experts du risque, leur opinion est souvent sollicitée. Toutefois il est primordial que la direction reconnaisse le cadre ERM et les processus de manière à ce que l'auditeur interne puisse donner un avis objectif sur l'efficacité du programme ERM.

LES COMPOSANTS DU CADRE

Un cadre ERM ne relève pas d'une seule et même politique mais d'un ensemble de composants, émanant de l'organisation, œuvrant ensemble à l'administration du risque dans la durée et de façon probante. Il incombe à l'auditeur de vérifier que la somme de ces composants constitue un cadre adéquat pour l'entreprise. La société Interis Consulting a développé un modèle ERM conceptuel basé sur les pratiques d'administration du risque, des secteurs public, financier et autres, ainsi que sur des critères propres à l'administration du risque et aux normes de contrôle. Ce modèle conceptuel inclut les principaux éléments d'un cadre ERM efficace et durable: la mise en place d'un cadre, l'implémentation de pratiques et de processus pour évaluer et traiter les risques et le contrôle du cadre.

MISE EN PLACE DU CADRE Lors de l'audit d'un cadre ERM, les auditeurs se doivent d'être vigilants quant aux lignes de conduite et aux valeurs établies sur l'administration du risque dans la politique de l'entreprise, quant au cadre de gouvernance et aux processus et outils d'administration du risque. Bien que les auditeurs ne soient pas impliqués dans la mise en place du cadre, puisque cela incombe à l'entreprise elle-même, ils sont cependant amenés à en évaluer les éléments au cours de l'audit. Dans certaines entreprises, les auditeurs trouveront des éléments du cadre qui intègrent des valeurs explicites d'administration du risque, des procédures d'administration du risque précises et claires à l'attention du personnel et des programmes de formation intensifs d'administration du risque. Dans d'autres entreprises, il peut s'avérer plus difficile pour le personnel d'identifier les pratiques afférentes à l'administration du risque, d'autant plus si le programme ERM est récent dans l'entreprise. Les auditeurs devront adapter les termes employés pour s'assurer que les employés comprennent la signification du concept d'administration du risque dans un environnement professionnel. Dans ce cas de figure, il est très important de tenir compte des signes multiples distinctifs pour s'assurer qu'un programme ERM sous-jacent, à savoir des pratiques d'administration du risque non identifiées en tant que telles au sein de l'entreprise, n'a pas été négligé par la direction.

Une fois le cadre défini, ses éléments sont mis en application par l'entreprise et l'administration constante du risque d'être menée, tout en évaluant et gérant les risques de façon constante. À charge ensuite des auditeurs de démontrer le bon fonctionnement et la mise en œuvre des pratiques définies en matière d'administration du risque.

ÉVALUATION DES RISQUES Durant l'audit des processus continus d'administration du risque, les auditeurs doivent vérifier que les objectifs de l'entreprise sont clairement définis et répertoriés. Le personnel de l'entreprise doit, lui, être au faîte de ces objectifs afin de gérer les risques qui y sont liés. Les auditeurs doivent ensuite vérifier s'il existe un processus pertinent d'identification du risque englobant tous les types de risque auxquels l'entreprise est exposée de manière inhérente et si ce processus est fondé sur une analyse de l'environnement de l'entreprise. Ils doivent également déterminer s'il existe un processus officiel d'évaluation du risque, si l'exposition à un risque résiduel a été mesurée par rapport à la tolérance au risque prescrite par la direction et s'il existe une procédure officielle de réponse au risque répertoriée et transmise.

Bien que les auditeurs ne soient pas impliqués dans la mise en place du cadre ERM, laquelle est du ressort de l'entreprise elle-même, ils évaluent les éléments de ce cadre au cours de l'audit.

TRAITEMENT DES RISQUES Dans leur processus d'évaluation du risque et la vérification de son efficacité, les auditeurs doivent définir la marche à suivre dans l'administration des risques dit «inacceptables», entre autres les mesures d'atténuation du risque, les délais et les responsables. Ces plans d'actions doivent faire l'objet d'un examen régulier et leur efficacité d'être contrôlée pour une atténuation du risque. Les personnes chargées de l'administration du risque au sein de l'entreprise doivent identifier et contrôler régulièrement les principaux indicateurs de ce risque, afin d'en détecter les premiers signes de matérialisation. Enfin, les auditeurs doivent s'assurer de la mise en

place de données et d'une terminologie normalisée dédiée à l'administration du risque.

CONTRÔLE DU CADRE Une entreprise doit être dotée de processus et de pratiques permettant le contrôle de l'efficacité du cadre ERM. En général, un auditeur doit rechercher des objectifs et des indicateurs pré-établis pour comparer les processus et le cadre ERM. Si l'objectif est de recouvrir la totalité des risques au sein de l'entreprise, un indicateur peut être le nombre de secteurs ayant un profil à risque. Les auditeurs doivent déterminer si la direction contrôle ce cadre pour s'assurer du bon fonctionnement des processus et s'il existe un contrôle indépendant de la qualité de l'administration du risque et de la diligence raisonnable dans la prise de décision en matière de risque.

LE PROCESSUS D'AUDIT

Bien que les audits d'un cadre ERM soient similaires à d'autres, dans leur processus de base, ils diffèrent cependant en raison de la nature unique de chaque cadre. Les auditeurs doivent être à même d'évaluer si un cadre répond aux attentes d'une entreprise.

ÉTENDUE D'APPLICATION Étendue d'application L'étendue d'application est une composante essentielle dans un audit mais elle l'est encore plus dans le cas d'un cadre ERM car les activités d'administration du risque sont regroupées en une fonction étendue qui souvent n'est pas désignée en tant que l'administration du risque. Par exemple, une entreprise peut disposer d'un manuel de procédures pour gérer les risques qui n'est pas désigné en tant que tel. Chaque entreprise repose sur des combinaisons différentes de systèmes, d'individus et de technologies pour identifier et gérer les risques dont les auditeurs doivent examiner tous les aspects. L'audit d'un programme ERM doit parfois inclure la vérification du programme de formation opérationnel si l'administration du risque fait partie de cette formation. Les auditeurs internes comprendront mieux les objectifs, les processus, la maturité, les conditions de travail et le profil de risque d'une entreprise en étudiant ses principaux aspects tels que :

- ses objectifs, sa mission, ses programmes et services et ses principaux résultats.
- les principales parties prenantes au sein de l'entreprise et en dehors y compris les ressources, les clients et les fournisseurs.
- les principaux processus de travail et les systèmes de contrôle mis en place pour atteindre les objectifs de l'entreprise et poursuivre sa mission.

Les auditeurs tendent à démontrer, dans la mesure du possible, la pérennité et la fiabilité des pratiques de l'entreprise et ce, grâce aux indicateurs permettant de gérer le risque efficacement.

- les cycles économiques des programmes, les services et activités essentielles, et leur interaction avec les autres cycles économiques.
- les lieux de mise à disposition des services et des programmes.
- les conditions dans lesquelles les programmes et les services sont fournis (par ex., économique, législatif, politique ou juridique).
- les tendances ou la stabilité des facteurs précités.

Il est essentiel que l'auditeur ait une connaissance parfaite de l'exposition de l'entreprise aux risques et aux menaces ainsi que de son historique. Par exemple, dans le cadre de l'audit du ministère d'un gouvernement important, les auditeurs d'Interis ont passé le premier tiers de leur mission à planifier, étudier et comprendre le contexte pour assimiler l'approche philosophique du risque et des risques élevés qui menaçaient les activités de ce secteur. Une fois qu'ils eurent acquis de solides connaissances de base de l'organisation, les auditeurs ont dissocié les segments principaux, tels que les fonctions opérationnelles et les ressources humaines et ont réduit l'étendue d'application de l'audit à trois segments, là où l'administration du risque était la plus concentrée. Des membres de l'équipe ont été affectés à chacun de ces secteurs pour en apprendre le plus

Principes directeurs des cadres ERM

Bien qu'ils puissent être de nature différente, en fonction des objectifs de l'entreprise, trois principes directeurs sous-tendent un cadre ERM sain.

- *Les pratiques ERM ont évolué en même temps que les objectifs et le contexte de l'entreprise ; il en va de même pour son profil de risque. Le cadre est par conséquent bien adapté aux activités distinctes de l'entreprise, à ses objectifs et à ses risques.*
- *Les pratiques ERM font corps avec tous les segments importants de l'entreprise, ainsi qu'avec les procédures et les lignes directrices et sont, de fait, soutenues par des outils efficaces d'évaluation, de communication et de contrôle du risque.*
- *Les pratiques ERM au sein de l'organisation doivent se renforcer conjointement et s'assurer que les groupes impliqués dans les activités liées au risque tendent vers le même objectif. Pour atteindre ce niveau d'intégration, les groupes doivent avoir une compréhension limpide des processus d'administration du risque de chacun, des buts et des méthodes ainsi que des responsabilités liées à l'administration du risque. L'ERM utilise les systèmes et les contrôles déjà en place au sein de l'entreprise dans sa gestion du risque.*

Les entreprises sont de plus en plus conscientes de la valeur générée par la pratique d'administration du risque; une valeur qui ne peut être générée qu'à travers la fiabilité du cadre.

possible sur les procédures et les processus mais aussi sur les outils utilisés dans le programme ERM qui ont permis de concevoir et de la mission d'audit.

OBJECTIFS ET CRITÈRES Au cours de l'évaluation du cadre ERM, l'auditeur tend à démontrer la fiabilité et la viabilité des processus en place, grâce aux indicateurs de risque qui permettent à l'entreprise de formuler une réponse adéquate et efficace. Lors du développement des objectifs et des critères d'audit, les auditeurs doivent :

- Concevoir un modèle conceptuel de cadre ERM adapté au contexte de l'entreprise. Par exemple, il est probable qu'une entreprise qui vient de mettre en place un programme d'administration du risque n'obtienne pas de résultats au niveau d'un programme de contrôle.
- Aligner les critères d'audit sur les quatre composantes du modèle de cadre ERM. L'audit d'un nouveau programme d'administration du risque tendra à spécifier les critères de contrôle basés sur l'existence d'une stratégie de contrôle plutôt que sur les résultats du programme de contrôle.
- Voir large dans la définition de process, tels qu'attendus, afin de prendre en compte la capacité d'adaptation de l'entreprise, quant aux conditions de travail, ainsi que l'ensemble des pratiques afférentes à l'administration du risque.

Par ailleurs, les auditeurs doivent obtenir l'approbation de la direction concernant les critères d'audit au commencement de l'audit. Si la direction n'approuve pas les critères en fonction desquels l'évaluation est faite, elle sera réticente quant aux conclusions et recommandations qui en découleront.

MISE EN ŒUVRE La conduite d'interviews durant l'audit d'un cadre ERM requiert de l'expérience et une connaissance approfondie des pratiques générales de gestion car l'ERM englobe des pratiques associées à d'autres secteurs tels que la finance, la conformité, les opérations et la sécurité. Bien qu'il existe une large gamme de procédures, la plupart des auditeurs ont recours aux interviews et à l'examen de documents. La sélection des personnes interviewées doit être en accord avec les objectifs de risque de l'entreprise. Par exemple, si le programme ERM est destiné à être exhaustif, les auditeurs seront amenés à interviewer un grand nombre de responsables dans toute l'entreprise. Les auditeurs doivent adapter leurs questions en fonction des connaissances de leur interlocuteur et reformuler les termes inconnus. En jugeant la qualité des informations liées au risque, les auditeurs doivent prouver que l'incertitude lors de la prise de décisions est réduite du fait que la direction ait accès à des informations précises et pertinentes sur les possibles conséquences indésirables d'événements pouvant nuire aux objectifs de l'entreprise.

Un cadre correctement audité est l'assurance d'une administration du risque et de la capacité à mettre en œuvre les changements nécessaires en temps voulu tout en poursuivant les objectifs de l'entreprise.

Lors de l'audit d'un cadre ERM, les auditeurs doivent :

- *Être à l'écoute du client* . Les auditeurs doivent prendre le temps de comprendre les objectifs professionnels du client, l'environnement de la concurrence, l'exposition au risque et la tolérance au risque. L'audit d'un cadre ERM ne consiste pas à le comparer en fonction d'une liste de caractéristiques mais à s'assurer qu'il contribue à la réalisation des objectifs d'une entreprise. Par exemple, les auditeurs d'Interis ont préconisé un programme d'ERM à la directrice financière d'une société de logiciels afin qu'elle soit immédiatement avisée des retards de livraison de projet. Le fait d'être informée à temps lui permettait de prendre des dispositions pour compenser le délai de paiement d'un client en annulant des dépenses ou en s'efforçant de conclure plus rapidement d'autres projets pour réaliser le chiffre trimestriel prévu.
- *Considérer les cadres ERM comme des travaux en cours* Les cadres varient en fonction du contexte professionnel et de la maturité de l'entreprise. Pour établir des recommandations pertinentes, il est important de comprendre l'état de l'entreprise lors du dernier audit, son état actuel et son orientation. Par exemple, le nouveau ministère d'un gouvernement avait un niveau d'expertise ERM très élevé dans les secteurs opérationnels essentiels à son activité mais une très faible expertise dans les secteurs de gestion d'entreprise. En apportant leurs recommandations, les auditeurs d'Interis ont gardé à l'esprit que deux ans auparavant ce ministère ne comportait pas de cadre ERM et que le point important était d'examiner le parcours réalisé par ce ministère pour mettre en place un cadre ERM solide et d'apporter les meilleures recommandations pour accélérer sa progression dans les secteurs les plus faibles.
- *Reconnaître que l'ERM peut prendre des aspects différents* Certaines entreprises ont un programme d'ERM intégré dans des systèmes. Par exemple, les institutions financières prescrivent généralement des lignes directrices précises à leurs employés sur les benchmark qu'un client doit remplir pour solliciter un produit ou un service. D'autres entreprises autorisent une grande marge de manœuvre à leurs dirigeants.
- *Rechercher les pratiques ERM dissimulées* L'administration du risque n'est pas un concept nouveau mais il se peut qu'au sein d'une entreprise, elle ne soit pas désignée en ces propres termes, surtout si le cadre ERM en est à un stade initial. Les auditeurs expérimentés examinent les procédures, les unités fonctionnelles comme les ressources humaines et les paramètres opérationnels pour

détecter les signes d'un programme d'ERM intégré. Si les cadres dirigeants peuvent répondre à la question, « Comment savez-vous quand …? », cela signifie qu'il existe une procédure ou une pratique soutenant un programme d'ERM. En fait, les pratiques d'administration du risque sous-jacentes dans tous les aspects d'une entreprise peuvent même être le signe d'un cadre ERM avancé et le programme d'ERM d'être tellement intégré à l'environnement de travail, que le personnel n'en a même pas conscience, pour ce qui est des termes liés au risque.

Lors de l'évaluation d'un cadre ERM, il est important que les auditeurs soulignent que l'ERM ne doit pas être mis en place simplement pour respecter la conformité réglementaire. L'objectif premier des auditeurs est donc de s'assurer que la vraie fonction de l'ERM est efficace quant à sa capacité à englober l'ensemble des décisions prises dans tous les secteurs de l'entreprise,

RAPPORTS La tâche la plus difficile, lors de l'audit d'un cadre ERM, est de tirer des conclusions et de faire des recommandations. Une fois que les résultats ont été collectés et rassemblés et ce, pour chaque critère, l'auditeur étudie dans quelle mesure le cadre ERM de l'entreprise répond aux objectifs. Les recommandations d'un audit doivent être raisonnables et réalisables et tenir compte du profil de risque et des objectifs de l'entreprise.

En rédigeant le rapport d'audit, les auditeurs doivent décrire le contexte de l'entreprise de manière explicite et précise de façon à ce qu'il serve de référence aux lecteurs du rapport au moment d'interpréter les résultats. Il est bon de schématiser les éléments relevés pour chaque recommandation de manière à ce que celles-ci soient toujours au plus près du profil de risque et des objectifs de l'entreprise. De cette façon, le rapport fera foi de l'état actuel du cadre ERM de l'entreprise et sera un bon moyen de mettre en application les recommandations.

TROUVER UN ÉQUILIBRE

Un cadre ERM correctement audité est l'assurance de l'administration des risques par une entreprise et de sa capacité à mettre en œuvre les rectifications nécessaires, en temps voulu, alors qu'elle poursuit ses objectifs. Il constitue aussi une base solide pour la prise de décisions. Parce que les audits d'ERM doivent s'adapter à la nature distincte des cadres ERM, une série de pratiques exemplaires peut être utile à l'évaluation du programme d'ERM en cours. Finalement, l'avenir de l'ERM réside dans l'intégration les cadres ERM aux activités quotidiennes. Parallèlement, les auditeurs continueront de jouer un rôle essentiel en contribuant au développement d'un cadre au sein de leur organisation et qui répond à ses attentes.

Pour commenter cet article, envoyez un courriel à l' auteur à alexandra.psica@theiia.org.

Cet article de Internal Auditor, l'édition le 2008 avril, est publié avec le permission de l'éditeur, The Institute of Internal Auditors. L'article été traduit de l'anglais à français.