La fraude et le contrôle interne – Première partie : l'importance des contrôles

Par EVERETT COLBY, CFE, FCGA

Le présent document est le premier d'une série de trois articles sur la fraude et le contrôle interne que M. Colby signera dans le Reper.

Ce premier article vise à faire ressortir combien il est important pour une société de mettre en place des contrôles en vue de se prémunir contre certains risques, à examiner les divers types de risques auxquels les sociétés sont exposées de nos jours, à souligner l'importance de la protection des données, à expliquer pourquoi les entreprises doivent mettre en place des systèmes de contrôle interne rigoureux pour prévenir et détecter les activités frauduleuses et à analyser la façon dont les CGA peuvent contribuer à l'amélioration de l'environnement de contrôle.

Introduction

De nos jours, les entreprises sont exposées à divers risques. Le risque de perte découlant d'une fraude figure parmi les risques les plus importants. Et ce risque s'intensifie rapidement pour les entreprises de toutes tailles. Les fraudes peuvent être d'origine interne, externe ou à la fois interne et externe. Selon de nombreux spécialistes de la fraude, le meilleur moyen de réduire au minimum le risque de perte découlant d'une fraude, de même que les autres risques, consiste à concevoir des contrôles internes qui protégeront les actifs et les ressources de l'entreprise et qui feront en sorte qu'il sera difficile de commettre ou de camoufler des activités frauduleuses.

L'importance des contrôles

En règle générale, la notion de « contrôle interne » n'a pas de secret pour les comptables, dont le travail s'appuie essentiellement sur la prémisse que les contrôles internes d'une entreprise aident celle-ci à s'assurer que ses résultats financiers sont comptabilisés adéquatement. Dans le contexte commercial actuel, les diverses menaces à la viabilité des entreprises et le risque de fraude gagnent beaucoup en importance. Il est toutefois possible de concevoir des contrôles internes, ou d'améliorer les contrôles en place, de manière à compliquer la tâche de ceux qui souhaitent commettre ou camoufler une fraude et à assurer la protection des actifs de la société ainsi que l'exactitude, l'intégrité et la sécurité des ressources des systèmes. Les contrôles internes doivent cependant porter sur l'ensemble des activités d'exploitation et de gestion de l'entreprise et non pas seulement sur les fonctions liées à l'information financière. Pour offrir un supplément de sécurité, il est en outre essentiel que le système de contrôle interne soit dûment appliqué.

Certains conseillers en sécurité et spécialistes de la fraude comparent le cadre commercial actuel, axé sur la technologie, à une « course à l'armement ». Les entreprises continuent de s'appuyer lourdement sur la technologie pour leur exploitation et leurs autres activités, mais le paysage technologique est en évolution et en expansion constantes. L'expression « course à l'armement » décrit bien la course entre ceux qui tentent de protéger les systèmes technologiques des entreprises et ceux qui tentent de compromettre ces mêmes systèmes.

L'évolution technologique a fait passer les entreprises des gros ordinateurs centraux aux serveurs de réseaux et des ordinateurs de bureau aux ordinateurs portables qui permettent une plus grande mobilité du personnel. Nous avons également assisté à l'avènement d'Internet et du commerce électronique, lequel tire parti d'Internet. Grâce à ces percées technologiques, l'information et les ressources autrefois conservées à l'intérieur de l'organisation (les gros ordinateurs centraux et les ordinateurs de bureau) sont maintenant accessibles de l'extérieur de l'organisation (serveurs de réseau et ordinateurs portables), à partir de n'importe où dans le monde (Internet et commerce électronique).

Tout le sens de cette course à l'armement « technologique » devient manifeste pour les entreprises lorsqu'elles constatent que, souvent, les contrôles visant à protéger leurs systèmes et leurs ressources ne sont pas conçus aussi rapidement que les systèmes en question. Ce décalage entre la mise en œuvre des innovations technologiques et la mise en place des systèmes de contrôle crée une brèche, et c'est là que des gens malhonnêtes peuvent causer de sérieux dommages.

Les risques auxquels les entreprises sont exposées

Les exigences des entreprises à l'égard des systèmes de comptabilité et d'information sont de plus en plus grandes. Pour répondre aux besoins d'information des entreprises, les systèmes sont donc de plus en plus complexes. Le contrôle de la sécurité et de l'intégrité de ces systèmes revêt donc, lui aussi, une plus grande importance. Les risques liés aux systèmes de comptabilité et d'information des entreprises sont variés, mais ils peuvent être regroupés en quatre grandes catégories distinctes :

- ***Catastrophes d'ordre naturel et politique*** — Cette catégorie comprend les actes terroristes, les tremblements de terre, les inondations et les incendies. Elle comprend également la possibilité d'actes terroristes ou d'instabilité politique dans des territoires étrangers où l'entreprise exerce des activités.
- ***Défaillances des systèmes*** — Cette catégorie comprend généralement les défauts de fonctionnement des ordinateurs et les erreurs de programmation, de même que les défaillances du matériel, les pannes de courant et les erreurs non détectées dans la transmission des données.
- ***Erreurs et actes non intentionnels*** — Cette catégorie englobe essentiellement les erreurs humaines et les accidents causés par la négligence humaine, les manquements à la procédure et les lacunes aux chapitres de la formation et de l'encadrement du personnel.
- ***Fraudes*** — Cette catégorie comprend les risques découlant d'actes intentionnels visant à priver l'entreprise de ses ressources ou de ses actifs.

Le profil de risque n'est pas le même pour toutes les entreprises. Certaines entreprises sont exposées à un niveau de risque plus faible que les autres entreprises dans une catégorie et à un niveau de risque plus élevé dans une autre catégorie. Ces écarts s'expliquent par divers facteurs, notamment le lieu où l'entreprise exerce ses activités, le degré de dépendance à l'égard des ressources technologiques et la nature des contrôles mis en place pour réduire au minimum l'exposition aux divers risques.

La nécessité de protéger les données

Compte tenu des risques décrits ci-dessus et du fait que les entreprises s'appuient de plus en plus sur les systèmes informatiques, il est de toute première importance de contrôler et de protéger ces systèmes. Toutes les entreprises, grandes et petites, sont exposées à certains des risques mentionnées ci-dessus, sinon à tous ces risques, et il ne fait aucun doute que les risques liés aux systèmes informatiques ne font que croître. Plusieurs études menées au cours des dix dernières années se sont intéressées aux raisons pour lesquelles les risques liés aux systèmes informatiques continuent particulièrement de s'intensifier. Voici les raisons les plus couramment invoquées :

- L'accroissement du nombre de systèmes client-serveur met l'information à la disposition d'un plus grand nombre de personnes.
- Comme les réseaux locaux et les systèmes client-serveur diffusent des données à un grand nombre de personnes, ils sont nettement plus difficiles à contrôler.
- Les réseaux longue portée (WAN) permettent aux clients d'avoir accès aux systèmes et aux données de leurs fournisseurs, et vice versa.
- L'utilisation d'Internet pour conclure des opérations commerciales donne à des personnes des quatre coins du monde la possibilité d'avoir accès à des données délicates.

Les données de l'entreprise sont sans contredit la composante des systèmes informatiques qui exige la plus grande protection. Les entreprises doivent comprendre que les données sont une ressource stratégique et que leur protection doit représenter une priorité stratégique. Nombre d'entreprises feraient faillite si des données essentielles cessaient d'être accessibles pendant une courte période. Les données d'une entreprise peuvent également présenter un intérêt certain pour ses concurrents. Les listes de clients, les données sur la conception des nouveaux produits et les listes de prix sont des exemples de documents très prisés qui ne sont souvent pas suffisamment protégés.

Malgré l'intensification des risques auxquels sont exposés les systèmes informatiques et l'information vitale, nombre d'entreprises ne protègent pas adéquatement leurs données. Le plus souvent, les raisons invoquées pour expliquer les lacunes au chapitre de la protection reposent sur des perceptions plutôt que sur des faits. Les problèmes pouvant découler des lacunes des contrôles informatiques sont souvent sous-estimés ou minimisés, particulièrement au sein des petites entreprises qui croient que seules les grandes entreprises sont exposées au risque. Dans bien des cas, ces entreprises ne se sentent pas concernées par le risque de perte de données vitales. Les répercussions sur le contrôle du passage d'un système centralisé à un système en réseau ne sont pas toujours bien comprises. Nombre d'entreprises ne comprennent pas que la sécurité des données est essentielle à leur survie. Finalement, de nombreuses sociétés estiment que les avantages de la protection demeurent inférieurs aux coûts.

Pour devenir plus proactives sur le plan de la sécurité et de la protection des données, les entreprises doivent fournir de l'information à leurs employés sur les mesures de contrôle et la protection des données. Certaines sociétés commencent à établir des politiques bien structurées, en matière de sécurité des données, en intégrant les contrôles de sécurité au processus même d'élaboration des applications.

Toujours sur le plan de la protection des données, les sociétés devraient envisager de transférer les données délicates emmagasinées sur des serveurs non protégés vers des environnements plus sécuritaires. Elles devraient également limiter l'accès aux données délicates et aux serveurs non protégés. En outre, comme les objectifs du contrôle interne sont les mêmes quelle que soit la méthode de traitement des données utilisée, des politiques et procédures différentes doivent être adoptées à l'égard des systèmes informatiques. Finalement, il est plus difficile d'opérer une séparation des tâches incompatibles dans un environnement informatisé que dans un environnement traditionnel. Il ne faut pas oublier que la responsabilité d'ensemble de la sécurité du système incombe à la haute direction. Cette

dernière doit diriger par l'exemple et ne pas passer outre aux contrôles en place. L'intégrité de tous les systèmes de contrôle interne repose sur une application indéfectible.

La contribution des CGA

Les CGA peuvent contribuer de deux façons à la modification de l'environnement de contrôle. D'abord, ils sont souvent appelés à participer à la conception ou à l'amélioration des systèmes de contrôle interne, soit à titre de conseillers indépendants, soit à titre de contrôleurs de la société. Grâce à leur formation, les CGA ont une excellente compréhension du fonctionnement des environnements de contrôle traditionnels, de leurs objectifs et de leur conception. Bien conscients du fait qu'il faut améliorer les environnements de contrôle pour réduire au minimum ou éliminer les divers risques et menaces, les CGA sont particulièrement bien placés pour faciliter la mise en place des changements qui s'imposent.

Les CGA exerçant en cabinet peuvent également favoriser la mise en place de changements au chapitre de l'environnement de contrôle par l'intermédiaire de leurs activités de vérification. En qualité de vérificateur, vous procédez toujours à une évaluation de l'environnement de contrôle interne de l'organisation, généralement dans le but d'estimer la probabilité que les résultats financiers que vous vérifiez contiennent des inexactitudes. En vertu des nouvelles exigences du *Manuel de l'ICCA*, le vérificateur doit également évaluer la probabilité de fraude au sein de l'organisation. Compte tenu des nouvelles exigences et du fait que le vérificateur signale généralement à l'organisation les lacunes constatées, les CGA devraient, au cours de leur examen du système de contrôle interne, chercher à déterminer si l'organisation a mis en place des contrôles adéquats en vue de protéger ses actifs et les ressources de ses systèmes contre tous les risques et toutes les menaces.

Conclusion

Comme les menaces et les risques auxquels sont exposés les actifs et les ressources vitales des entreprises se font de plus en plus importants, la mise en place de contrôles est désormais essentielle. Jusqu'ici, les contrôles internes étaient généralement conçus en vue d'assurer l'exactitude des résultats financiers présentés par l'organisation. Étant donné l'intensification des risques, et particulièrement du risque de fraude, ces contrôles doivent également être conçus en vue de compliquer la tâche de ceux qui souhaitent commettre ou camoufler une fraude et de réduire au minimum le risque de perte pouvant découler de divers types de menaces.

De nos jours, les risques auxquels sont exposées les entreprises sont variés et ils se multiplient plus rapidement que par le passé. Parmi ces risques, mentionnons les catastrophes d'ordre naturel ou politique, les défaillances des systèmes, les erreurs et les actes non intentionnels ainsi que la fraude. S'il importe tant que les entreprises améliorent leurs contrôles, c'est parce que ce faisant elle seront mieux en mesure de réduire au minimum les pertes pouvant découler des divers risques auxquels elles sont exposées. En outre, compte tenu de l'utilisation accrue d'Internet et des réseaux client-serveur, l'information vitale des entreprises est de plus en plus menacée. En effet, s'il est désormais plus facile d'accéder aux données, il est en revanche plus difficile de les protéger. Jamais la protection des données vitales de l'organisation n'aura été aussi cruciale.

Or, malgré l'importance des données, de nombreuses entreprises négligent encore de se protéger adéquatement. Nombreuses sont celles qui estiment que les menaces ou les risques liés aux données sont minimes ou que la sécurité des données n'est pas essentielle à leur survie. D'autres font valoir que les avantages demeurent inférieurs aux coûts. Elles n'ont pas compris que les données constituent une ressource stratégique et que leur protection devrait représenter une priorité stratégique. Essentiellement, la responsabilité de la protection des systèmes et des données vitales de l'organisation incombe à la haute direction et, pour être efficaces, les contrôles doivent être dûment appliqués.

Dans la deuxième partie de cette série de trois articles, nous proposerons une méthode pour vous aider à concevoir des contrôles permettant d'atténuer les risques. Dans la troisième partie, nous discuterons des stratagèmes de fraude les plus courants et des indices de leur existence. Il est plus facile de concevoir des contrôles visant à atténuer les risques de fraude lorsqu'on comprend comment la fraude est perpétrée.

Praticien exerçant en cabinet, Everett Colby, CFE, FCGA, est propriétaire de l'un des bureaux de Porter Hétu International, l'un des 30 premiers cabinets comptables en importance du Canada selon le magazine The Bottom Line. *M. Colby est également propriétaire de North American Forensic Accountants and Fraud Investigators Inc., un cabinet de juricomptabilité. Il est membre du conseil d'administration de CGA-Ontario, président du Comité d'étude de la politique fiscale et budgétaire de CGA-Canada et membre à vie de l'International Association of Certified Fraud Examiners. M. Colby anime régulièrement des ateliers, au Canada et à l'étranger, sur des sujets comme la fraude, le blanchiment d'argent, les sanctions civiles et l'éthique dans le contexte commercial actuel.*

Ce document est le premier d'une série de trois articles sur la fraude et le contrôle interne que M. Colby signera dans le Reper.