

Nouvelles normes techniques pour les audits financiers : Comment les auditeurs informatiques réunissent des éléments probants afin d'évaluer les contrôles internes

Tommie Singleton, Ph. D., CISA, CMA, CPA, CITP

Il est incontestable que l'importance accordée à l'évaluation des contrôles internes intégrés dans les systèmes informatiques et les technologies de l'information (TI) s'est considérablement accrue au cours des cinq dernières années. Les auditeurs ont donc une responsabilité de plus en plus accrue de comprendre les contrôles internes et de les évaluer. Le présent article contient un bref historique de l'évolution de l'accent mis sur les contrôles internes et propose certains conseils pratiques de base sur la façon dont les auditeurs informatiques peuvent jouer leur rôle et s'acquitter de leurs responsabilités en ce qui concerne l'évaluation des contrôles internes. L'article porte plus précisément sur un cadre qui permettrait aux auditeurs informatiques d'évaluer les contrôles internes au sens large, c'est-à-dire l'évaluation de l'environnement de contrôle.

Historique des normes et des règlements encadrant les contrôles internes

Certaines lois comme les lois sur les valeurs mobilières de 1932 et de 1933 et le *Foreign Corrupt Practices Act* de 1977 aux États-Unis contenaient déjà des dispositions sur les contrôles internes. Les normes d'audit de l'American Institute of Certified Public Accountants (AICPA) exigent quant à elles une évaluation du risque lié au contrôle (p. ex., la « formule d'audit ») depuis des années. Au début des années 1960, l'évaluation des contrôles est devenue plus complexe, l'utilisation des systèmes comptables informatisés se répandant.

La tendance actuelle en matière de réglementation sur les contrôles internes émane cependant de la Treadway Commission et de son Committee on Sponsoring Organizations (COSO). La Treadway Commission avait été chargée d'élaborer une stratégie ou une méthode qui pourrait contribuer à endiguer la vague de scandales qui a déferlé sur le secteur de l'épargne et du crédit dans les années 1980. Selon la Treadway Commission, la meilleure façon d'éviter que de tels scandales se reproduisent était d'instaurer un modèle complet de contrôles internes. Le modèle qui en est résulté, le référentiel COSO, a été adopté par les organisations membres du COSO : l'American Accounting Association, Financial Executives International, l'Institute of Management Accountants, l'Institute of Internal Auditors et l'AICPA.

Le référentiel COSO est essentiellement un cadre de réflexion, d'analyse ou d'établissement d'un système efficace de contrôle interne. Il comporte cinq composantes : l'environnement de contrôle, l'évaluation des risques, la communication et l'information, le suivi et les activités de contrôle. Au début des années 1990, l'AICPA a érigé le référentiel COSO au rang de norme technique pour les audits financiers et l'a incorporé dans le Statement on Auditing Standards (SAS) No. 78, *Consideration of Internal Control in a Financial Statement Audit*.

Les fraudes financières des dix années qui ont suivi ont rehaussé l'importance accordée aux contrôles internes, tout comme la promulgation de la *Sarbanes-Oxley Act of 2002* (la « loi Sarbanes-Oxley ») aux États-Unis. La plupart des intéressés conviennent que cette loi est une conséquence directe des fraudes financières d'Enron et de WorldCom. L'article 404 de la loi

Sarbanes-Oxley exige que la direction fasse une évaluation des contrôles internes et que les auditeurs financiers expriment une opinion sur cette évaluation. La loi Sarbanes-Oxley a également donné lieu à la création du Public Company Accounting Oversight Board (PCAOB), organisme relevant de la Securities and Exchange Commission (SEC) des États-Unis et chargé d'assurer la surveillance de l'information financière des sociétés cotées.

Le PCAOB est le principal organisme de normalisation en ce qui a trait à l'information financière. La première norme publiée par le PCAOB avalisait toutes les normes précédentes concernant l'information financière. La deuxième, l'AS2, portait sur la conformité à l'article 404 de la loi Sarbanes-Oxley. Le PCAOB y reconnaissait le référentiel COSO comme un moyen efficace pour comparer et évaluer les contrôles internes.

Dans le courant de cette même année, l'AICPA a publié le SAS No. 99, *Consideration of Fraud in a Financial Statement Audit*, dans lequel étaient codifiés certains objectifs de la loi Sarbanes-Oxley et certaines des pratiques professionnelles exemplaires en matière de lutte contre la fraude (à titre d'outils et de méthodes pour ces dernières).

L'année dernière, l'AICPA a publié le SAS No. 109, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement*. Si le titre peut porter à confusion, le sous-titre indique clairement que, collectivement avec le SAS No. 100, le SAS No. 109 remplace le SAS No. 55, *Consideration of Internal Control in a Financial Statement Audit*. Autrement dit, ces deux normes constituent le plus récent référentiel technique sur le sujet du contrôle interne dans un audit financier.

Effet des lois et des textes récents concernant le contrôle interne sur les auditeurs informatiques

La grande majorité des contrôles internes étant à présent intégrés dans les systèmes automatisés ou les TI, les auditeurs informatiques sont devenus un élément essentiel de la conformité aux normes, aux lignes directrices et aux règlements.

Toutes les parties intéressées à l'audit connaissent les faits historiques, les lois et les textes se rapportant aux contrôles internes qui sont mentionnés précédemment. Les quatre grands cabinets comptables et les sociétés cotées du Fortune 500 ont mis en œuvre des procédures d'audit informatique efficaces et ont fait appel à des auditeurs informatiques pour se conformer à ces normes et règlements.

Des entités autres que les grandes sociétés cotées commencent toutefois à s'intéresser aux exigences de la loi Sarbanes-Oxley. Certains secteurs d'activité sont en voie de les adopter même s'ils ne sont pas légalement tenus de le faire. Le Congrès américain a en outre décrété que certains organismes publics, tels que la Tennessee Valley Authority, seront assujettis à la loi Sarbanes-Oxley. Certaines entreprises internationales ont dû faire des ajustements en raison de leurs relations avec des entreprises américaines. Il n'est donc pas rare que des cabinets d'audit, des services d'audit interne et des gestionnaires soient aux prises avec la question de la conformité, en particulier l'audit informatique des contrôles internes.

La profession d'auditeur a reconnu que bon nombre des contrôles internes à l'égard de l'information financière sont tributaires des contrôles des applications logicielles et des systèmes d'information. Cette dépendance est particulièrement vraie pour les contrôles de surveillance essentiels (p. ex., les évaluations de la performance). Par conséquent, il est de plus en plus nécessaire que les auditeurs financiers, en particulier les auditeurs informatiques qui participent à des missions d'audit financier, soient en mesure d'évaluer les risques associés aux TI, les contrôles automatisés et la longue liste de suggestions du SAS 109.

Audits informatiques et pratiques exemplaires

Évaluer des contrôles internes, c'est un peu comme peler un oignon : il faut le faire une couche à la fois. Une stratégie efficace consiste à commencer par les éléments les plus généraux de l'évaluation pour ensuite appliquer des procédures d'audit ciblées à des éléments précis. Le référentiel COSO propose une approche similaire, si les éléments sont traités par ordre chronologique. Le premier élément est l'environnement de contrôle : Comment l'auditeur informatique sait-il où se trouvent les risques dans l'environnement de contrôle, et comment obtient-il des éléments probants efficaces (reconnaissables) d'un « bon » environnement de contrôle?

Il existe des « pratiques exemplaires » pour plusieurs axes de fonctionnement des TI qui peuvent se révéler efficaces pour l'évaluation des contrôles internes. Le premier axe considéré est celui de la gouvernance des TI¹, qui fournit des principes et des outils pour fournir l'assurance aux parties prenantes que l'entité fait une utilisation efficiente et efficace de ses ressources par rapport à l'emploi de l'informatique. Si c'est le cas, une évaluation appropriée du niveau de gouvernance des TI de l'entité donnera une bonne mesure de l'environnement de contrôle de l'entité. Autrement dit, l'emploi des pratiques exemplaires de gouvernance des TI accroît le niveau d'assurance quant au fait que les systèmes utilisés comportent des contrôles internes efficaces et que l'environnement de contrôle est « bon ».

L'obtention d'éléments probants de la gouvernance des TI commence au niveau du conseil et/ou de la haute direction. Ainsi, l'entité emploie au moins une des pratiques exemplaires de gouvernance des TI si son conseil s'est doté d'un comité permanent sur les TI ou s'il a mis un point permanent sur les TI à l'ordre du jour de chacune de ses réunions. Le contenu des procès-verbaux (du conseil ou du comité sur les TI) fournit des éléments probants de l'efficacité du conseil en ce qui a trait à la gouvernance des TI. Les budgets, les politiques et les procédures, un organigramme de la structure organisationnelle stratégique qui comprend la séparation des tâches, et d'autres documents peuvent également servir d'éléments probants de l'emploi efficace des pratiques exemplaires de gouvernance des TI.

Nul mieux que la direction ne devrait connaître les risques associés au contrôle interne et aux anomalies significatives. Il est donc logique de commencer l'évaluation par ce niveau de l'organisation. Quelques textes du référentiel reposent sur un effet de causalité « descendant » (comme la célèbre expression « du ton donné par la direction » et son sens). Vu sa relation de

¹ L'IT Governance Institute^{MD} (ITGI^{MC}) est un chef de file de la gouvernance des TI. Pour de plus amples informations, veuillez visiter le site Web de l'ITGI, à l'adresse www.itgi.org.

proximité à la direction, l'environnement de contrôle a donc un effet d'entraînement sur d'autres aspects des contrôles internes (p. ex., évaluation des risques, suivi).

Le deuxième axe à considérer est celui de l'emploi des pratiques exemplaires concernant la gestion de projets². Celles-ci sont utiles pour s'assurer que les projets sont livrés à temps et dans le respect des budgets, et qu'ils sont entièrement fonctionnels selon les exigences du système. Bien souvent, le problème que posent les projets de TI a trait au fait qu'il n'existe pas de critères pour définir exactement ce qu'est un projet. L'instauration de pratiques exemplaires a une incidence sur l'environnement de contrôle : elle indique que le niveau de risque lié au développement du système (et aux contrôles qui y sont incorporés) est moindre et, partant, réduit le risque que les projets échouent et que l'entité doive radier les coûts engagés pour ces projets. La présence d'experts (employés agréés à titre de professionnels de la gestion de projets), d'un bureau de gestion de projets et de documentation sur les projets (p. ex., diagrammes de Gantt, ventilation des travaux) fournit elle aussi des éléments probants. L'auditeur informatique obtient une plus grande assurance que les contrôles internes sont efficaces si l'entité adopte des pratiques exemplaires en matière de gestion de projets.

Le troisième axe que l'auditeur informatique aimerait voir l'entité emprunter est celui des pratiques exemplaires liées au cycle chronologique de l'élaboration des systèmes (CCES)³. Chacune des phases de ce cycle est documentée et cette documentation fournit des éléments probants pouvant servir à déterminer si l'entité emploie les pratiques exemplaires liées au CCES. Une utilisation efficace des pratiques exemplaires concernant le CCES fournit à l'auditeur informatique une assurance quant au fait que l'environnement de contrôle est « bon ».

Pour les auditeurs financiers, les deux derniers axes (CCES et gestion de projets) se confondent parfois puisque tous les projets qui présentent un risque financier important ont trait au développement ou à la modification d'applications et à la conversion des données, et tous suivent les processus du CCES. Cependant, aux fins de l'évaluation des contrôles internes, les pratiques exemplaires touchant ces deux axes sont différentes.

Audits informatiques, contrôles internes et CobiT

Le présent article consiste essentiellement en une analyse générale des TI et des contrôles internes au niveau de l'environnement du contrôle. Une façon de structurer cette évaluation consiste à utiliser les objectifs de contrôle pour les technologies de l'information et les technologies connexes ou COBIT^{MD} (*Control Objectives for Information and related Technology*). Celui des quatre aspects qui s'applique le mieux à l'évaluation de l'environnement de contrôle est « Planifier et organiser » (PO).

Cet aspect concerne la stratégie et les tactiques et s'intéresse à la façon dont les TI peuvent le mieux contribuer à l'atteinte des objectifs d'affaires. Il traite aussi du fait que la réalisation de la

² La rubrique « IT Audit Basics » de l'*Information Systems Control Journal* (volume 5, 2006) traite du risque lié à la gestion de projets. Veuillez la consulter pour obtenir de plus amples informations sur l'évaluation des risques et la relation entre la gestion de projets et l'évaluation des contrôles internes.

³ La rubrique « IT Audit Basics » de l'*Information Systems Control Journal* (volume 1, 2007) porte exclusivement sur le CCES. Veuillez la consulter pour obtenir de plus amples informations sur l'utilisation du CCES pour évaluer les contrôles internes.

vision stratégique doit être planifiée, communiquée et gérée selon différents angles. Enfin, il repose sur le principe que la structure organisationnelle et l'infrastructure technologique en place doivent être adéquates.

L'aspect PO englobe 10 processus (voir la **figure 1**) qui peuvent servir de cadre à la collecte d'éléments probants sur l'environnement de contrôle. Les trois axes de fonctionnement des TI susmentionnés peuvent fournir des éléments probants concernant ces 10 processus. De plus, pour certains de ces processus, les pratiques exemplaires ayant trait à chacun des trois axes peuvent fournir des éléments probants quant au niveau d'assurance associé à l'environnement de contrôle. Au moins un des trois axes englobe les 10 processus.

Figure 1 : Processus couverts par l'objectif PO du COBIT	
PO1	Définir un plan stratégique des TI
PO2	Définir l'architecture de l'information
PO3	Déterminer l'orientation technologique
PO4	Définir les processus, l'organisation et les relations en matière de TI
PO5	Gérer l'investissement en TI
PO6	Communiquer les objectifs et l'orientation de la direction
PO7	Gérer les ressources humaines en TI
PO8	Gérer la qualité
PO9	Évaluer et gérer les risques liés aux TI
PO10	Gérer les projets

Par conséquent, en conjuguant l'aspect PO du COBIT, l'environnement de contrôle du référentiel COSO et les pratiques exemplaires en matière de gouvernance des TI et de gestion de projets ainsi que celles liées au CCEs, les auditeurs informatiques devraient être en mesure d'élaborer une stratégie efficace pour analyser l'environnement de contrôle. Une telle stratégie devrait leur permettre d'évaluer efficacement le niveau d'assurance que procurent les contrôles internes intégrés dans les TI en général.

Conclusion

Les auditeurs informatiques pourraient trouver que les aspects COBIT (en particulier l'aspect PO) et le référentiel COSO (en particulier le composant environnement de contrôle) sont des outils utiles pour évaluer les contrôles internes. De plus, en combinant les pratiques exemplaires des trois axes de fonctionnement des TI de l'entité, l'auditeur informatique peut, au minimum, acquérir une bonne compréhension de l'environnement de contrôle et probablement réunir une quantité substantielle d'éléments probants qui pourront lui être utiles pour pousser son évaluation des contrôles internes. Bien que l'étendue de cet article ait été volontairement limitée aux questions liées aux contrôles internes et à la conformité à l'article 404 de la loi Sarbanes-Oxley, au SAS No. 109 ou à l'AS2, il tente néanmoins d'illustrer l'utilité de ces techniques et outils pour le volet général de l'évaluation des contrôles internes.

Pour certains, l'audit commence et finit avec l'environnement de contrôle. Les auditeurs qui réalisent des audits financiers peuvent recourir à l'environnement de contrôle pour délimiter et comprendre les changements ayant eu lieu depuis la dernière évaluation, ainsi que pour déterminer les risques de niveau plus faible qui sont présents et la façon d'y répondre.

Selon l'évaluation qu'il fait de la gouvernance des TI, de la gestion de projets et/ou du CCES, l'auditeur informatique peut réunir des éléments probants qui lui permettront de déterminer si l'environnement de contrôle est approprié. Un environnement de contrôle approprié ne veut toutefois pas nécessairement dire que des contrôles internes sont incorporés dans les systèmes. Il indique plutôt que l'entité a décidé d'appliquer les pratiques exemplaires, ce qui suppose habituellement d'adopter une approche réfléchie pour d'autres aspects des TI, comme l'incorporation efficace de contrôles internes : c'est-à-dire qu'il y a habituellement un effet d'entraînement favorable sur les contrôles intégrés dans les processus des TI situés en aval de l'environnement de contrôle, qui représente le niveau le plus élevé dans l'entité.

D'autres aspects du référentiel COSO et du COBIT, ainsi que des tests de détail des contrôles fourniront des éléments probants supplémentaires de l'assurance que procurent les contrôles internes.

Tommie W. Singleton, Ph. D., CISA, CMA, CPA, CITP, est professeur agrégé en systèmes d'information à l'Université de l'Alabama à Birmingham (États-Unis). Il détient une bourse de recherche Marshall sur les systèmes d'information et il est aussi directeur du programme de juricomptabilité de cette université. Avant d'obtenir son doctorat en comptabilité à l'Université du Mississippi (États-Unis) en 1995, Tommie Singleton a été président d'une petite entreprise à valeur ajoutée spécialisée dans la vente de systèmes d'information comptable destinés aux micro-ordinateurs. En 1999, l'Alabama Society of CPAs lui a décerné l'Innovative User of Technology Award pour 1998-1999. Tommie Singleton est le porte-parole universitaire de l'ISACA à l'Université de l'Alabama à Birmingham. Ses articles sur la fraude, les TI/SI, l'audit informatique et la gouvernance des TI ont été publiés dans de nombreuses revues, y compris l'*Information Systems Control Journal*.

L'*Information Systems Control Journal*, anciennement l'*IS Audit & Control Journal*, est une publication de l'Information Systems Audit and Control Association, Inc. Le statut de membre de l'association, organisme réunissant des bénévoles s'intéressant à l'audit des systèmes d'information (SI), au contrôle et à la sécurité, s'accompagne d'un abonnement annuel gratuit à l'*Information Systems Control Journal*.

Les opinions exprimées dans l'*Information Systems Control Journal* sont celles des auteurs et des annonceurs. Elles peuvent être différentes des politiques et des déclarations officielles de l'Information Systems Audit and Control Association et de celles de l'IT Governance Institute^{MD} et de leurs comités, ainsi que des opinions approuvées par les employeurs des auteurs ou par les rédacteurs de l'*Information Systems Control Journal*. L'*Information Systems Control Journal* ne garantit pas l'originalité du contenu fourni par les auteurs.

© Copyright 2004. Information Systems Audit and Control Association Inc., anciennement l'EDP Auditors Association. Tous droits réservés. ISCA^{MC} Information Systems Control Association^{MC}

Source : *Information Systems Control Journal*, volume 4, Copyright © 2007 ISACA. Tous droits réservés www.isaca.org. Traduit par CGA-Canada et reproduit avec permission.