RÉSEAU **CANADIEN**
DES COMITÉS DE VÉRIFICATION
VantagePoint

Le 30 avril 2007

TAPESTRY NETWORKS, INC · WWW.TAPESTRYNETWORKS.COM · +1 781-290-2270

La gouvernance des technologies de l'information

Introduction

Le Réseau canadien des comités de vérification (RCCV) est un groupe sélect de présidents de comités de vérification de grandes sociétés canadiennes. Les réunions du RCCV, qui sont organisées par Ernst & Young et orchestrées par Tapestry Networks, visent à faciliter l'accès aux nouvelles meilleures pratiques ainsi que le partage des connaissances sur les principaux enjeux auxquels est confronté le secteur de la vérification, dans un contexte de transformations.

La troisième réunion du RCCV, qui s'est tenue à Toronto le 3 avril 2007, a porté sur les risques accrus et les nouvelles possibilités qui sont associés aux technologies de l'information.

Le présent document se veut une synthèse des principaux enjeux qui sont ressortis de cette réunion. Le principal mérite de la publication *VantagePoint* réside dans le fait qu'elle aide tous les membres du RCCV à préciser leur propre point de vue éclairé sur les enjeux importants auxquels ils sont confrontés. Tous ceux et celles qui l'ont reçue peuvent la mettre à la disposition des membres de leur propre réseau. Plus nous arriverons à diffuser largement l'information qu'elle contient auprès des administrateurs, des hauts dirigeants et de leurs conseillers, plus la valeur qui en découlera pour tout le monde sera importante.

En tout et pour tout, les membres du RCCV ayant participé à cette rencontre siègent au conseil d'administration de plus de trente sociétés ouvertes dont la capitalisation boursière va de faible à importante. Il s'agit des personnes suivantes :

- Mike Boychuk, président du comité de vérification du Fonds de revenu Pages Jaunes
- John Caldwell, président du comité de vérification de Cognos
- Denis Desautels, président du comité de vérification d'Alcan
- Don Fullerton, président du comité de vérification de Husky Energy
- Krystyna Hoeg, présidente du comité de vérification de Financière Sun Life
- Bob Luba, président du comité de vérification de MDS
- Tom O'Neill, président du comité de vérification de BCE
- Pierre Robitaille, président du comité de vérification de Les Vêtements de Sport Gildan

Étaient également présentes à la réunion, à titre de représentants d'Ernst & Young, les personnes suivantes :

- Anne-Marie Hubert, associée, Services consultatifs en risque (SCR), groupe canadien des Services en technologie et en risques de sécurité (STRS)
- Lou Pagnutti, associé directeur régional, et président et chef de la direction d'Ernst & Young Canada
- Rob Scullion, associé directeur du groupe Certification et services consultatifs aux entreprises d'Ernst & Young Canada

La publication *VantagePoint* reflète l'utilisation par le RCCV de la version modifiée des règles de Chatham House, en vertu desquelles le nom de ses membres et les liens qui les unissent à leur société sont de notoriété publique, la paternité des propos tenus au cours de réunions n'étant toutefois pas attribuée à des personnes ou à des sociétés.

Sommaire

Selon Ken Doughty et Frank Grieco, la gouvernance des TI est un cadre de gestion efficace et efficient des ressources informationnelles (qui englobent notamment les ressources humaines, le financement et l'information), dont le but est de faciliter la réalisation des objectifs de l'entreprise. Ce cadre de gestion est orienté vers l'évaluation et la gestion de la performance des TI, de façon à assurer un contrôle approprié des risques et des coûts relatifs aux TI.[1]

Les membres du RCCV conviennent que l'importance des TI sur les plans stratégique et opérationnel justifie que les conseils d'administration y accordent l'attention nécessaire. Compte tenu de l'importance des TI dans la présentation de l'information financière et l'application des contrôles, les comités de vérification sont souvent appelés à jouer un rôle de leadership dans la surveillance des TI. Dans le cadre de leurs discussions sur les risques et possibilités générés par les TI, les membres du RCCV ont traité la question de la répartition des responsabilités à cet égard entre le comité de vérification et le conseil d'administration dans son ensemble, en plus de recenser les sources spécialisées internes et externes auxquelles il est possible de faire appel.

- **Nécessité de prendre en compte à la fois les risques et les possibilités dans le cadre de la surveillance des TI** *(page 3)*

  Le déploiement de plus en plus étendu des systèmes de TI crée d'énormes possibilités, qui s'accompagnent de risques presque aussi importants. Des faiblesses insoupçonnées dans les contrôles de TI ont été mises en lumière dans le cadre de la mise en œuvre de l'article 404 de la loi Sarbanex-Oxley. Bien que la responsabilité à l'égard des risques liés à l'information financière incombe principalement au comité de vérification, le conseil d'administration doit également prendre en compte les incidences des TI sur la stratégie et les activités de l'entreprise.

- **Nécessité pour les conseils d'administration de veiller à une répartition appropriée des responsabilités à l'égard de la surveillance des TI** *(page 5)*

  Les membres du RCCV ont fait valoir la nécessité de bien répartir entre les administrateurs les responsabilités à l'égard de la surveillance des TI. La responsabilité à l'égard des systèmes de TI assurant la prise en charge de l'information financière incombe clairement aux comités de vérification. Néanmoins, comme ceux-ci assument déjà une lourde charge de travail, ils ne sont pas en mesure de prendre la responsabilité de l'ensemble des questions relatives aux TI. Dans les cas où les TI représentent un inducteur stratégique clé pour l'entreprise, les membres du RCCV croient qu'il revient au comité

[1] Ken Doughty et Frank Grieco, *IT Governance: Pass or Fail?*, *Information Systems Control Journal*, Volume 2, 2005. Document accessible à l'adresse suivante : http://www.isaca.org/Template.cfm?Section=JOnline&CONTENTID=24195&TEMPLATE=/ContentManagement/ContentDisplay.cfm

d'administration dans son ensemble de s'engager activement dans la surveillance de cet aspect. En revanche, lorsque le rôle des systèmes de TI ne consiste plutôt qu'à soutenir la stratégie de l'entreprise, ils ne croient pas que la participation de tous les administrateurs soit nécessaire.

- **Nécessité pour les conseils d'administration de s'appuyer sur des sources externes et internes spécialisées en TI** *(page 6)*

  S'il est vrai que les comités de vérification comptent peu de membres ayant une connaissance approfondie des TI, ils ont tout de même la possibilité de se tourner vers des spécialistes en la matière. Les vérificateurs externes, la fonction vérification interne et le chef de l'information sont en mesure de les orienter, de leur prodiguer des conseils et de les aider à établir la vision globale de la fonction TI. En outre, des membres du RCCV plaident volontiers en faveur de l'intégration au sein des conseils d'administration d'administrateurs ayant une meilleure connaissance des TI, de façon à ce que les questions pertinentes puissent être posées.

À l'issue de la réunion du RCCV, Ernst & Young a préparé à l'intention des administrateurs une longue liste de questions auxquelles ils sont invités à répondre dans le cadre de la poursuite de leurs divers objectifs en matière de gouvernance des TI. Ces questions portent notamment sur les sujets suivants : meilleur alignement entre l'entreprise et les TI, gestion des investissements en matière de TI axée sur la création de valeur, efforts visant la satisfaction des exigences en matière de conformité, évaluation de la performance, élaboration et mise en œuvre d'un cadre cohérent de gestion des risques, mise en place d'une gestion adéquate de l'entreprise et de ses ressources, nécessité d'assurer l'application par les tiers de pratiques de gouvernance efficaces. Cette liste figure en annexe, à la page 9.

Nécessité de prendre en compte à la fois les risques et les possibilités dans le cadre de la surveillance des TI

Les grandes entreprises sont tributaires de l'efficacité des TI en ce qui a trait à la prise en charge des systèmes opérationnels et des systèmes de contrôle complexes. Les systèmes essentiels à la réalisation de leur mission doivent fonctionner comme prévu et sans interruptions de services, et leurs systèmes d'information financière doivent générer en temps opportun une information exacte, fiable et sécurisée. C'est pour toutes ces raisons que la surveillance des TI représente de plus en plus un enjeu majeur pour les administrateurs de sociétés.

Non seulement les TI sont-elles de plus en plus une source de possibilités et de risques, elles gagnent également en importance du fait qu'une part considérable du budget des immobilisations est affectée à la mise en œuvre et à la mise à niveau des systèmes. Conscients de cette situation, les membres du RCCV s'inquiètent du trop peu d'attention accordée à la surveillance des TI par bon nombre de conseils d'administration. Souvent, les discussions sur les TI engageant l'ensemble du conseil d'administration ne portent que sur les dépenses en immobilisations, les enjeux plus larges liés à la gouvernance des TI étant pour leur part passés sous silence.

Les membres du RCCV conviennent que, dans une large mesure, les questions relatives à la gouvernance des TI peuvent être regroupées en trois catégories : l'information financière, l'exploitation et la stratégie.

- **Information financière –** À l'issue du processus d'attestation de l'efficacité de leurs contrôles, bien des sociétés se trouvent confrontées à des problèmes de TI qu'elles ne soupçonnaient même pas. Un article publié récemment dans *Compliance Week* révèle que les problèmes signalés vont des lacunes sur le plan de la sécurité à une répartition inadéquate des responsabilités, en passant par les déficiences relatives à la consignation des procédés et marches à suivre ainsi qu'au transfert manuel de données entre programmes ou applications, pour ne citer que quelques sources de tracas.[2] Les membres du RCCV se sont montrés surpris du grand nombre de procédés de remplacement manuels ayant été recensés dans leur propre entreprise. Certains ont le sentiment que, à bien des égards, l'entrée en vigueur de l'article 404 de la loi Sarbanes-Oxley représente ce qu'il pouvait arriver de mieux à leur comité de vérification. Les problèmes relatifs au contrôle des modifications apportées sur les plans de l'accès et des programmes, à la consignation des directives en matière de TI et à d'autres contrôles généraux tels que ceux se rapportant aux procédures de sauvegarde et de reprise, à la planification, et à la gestion des incidents et des problèmes font partie des aspects que les comités de vérification doivent prendre en considération. Selon les membres du RCCV, l'information financière et les risques de non-contrôle sont des éléments importants de tout cadre de gestion des risques à l'échelle de l'entreprise.
- **Exploitation** – Les entreprises dépendent de plus en plus des systèmes de TI pour assurer la prise en charge de leurs processus opérationnels essentiels à la réalisation de leur mission, notamment les processus relatifs à la fabrication, à la vente et à la gestion de la chaîne d'approvisionnement. Bien que ces activités ne se rapportent pas directement aux responsabilités qui incombent au comité de vérification à l'égard de la surveillance des TI, leur succès ou leur échec ne manquera pas d'influer considérablement sur les résultats financiers de l'entreprise. Les conseils d'administration doivent donc se poser des questions fondamentales : Pouvons-nous gérer les modifications apportées à l'environnement de TI sans exposer l'entreprise à des risques inacceptables? Sommes-nous en mesure de sécuriser les systèmes de l'entreprise de façon à les protéger contre les menaces internes et externes? Nos objectifs d'efficacité et de rentabilité sont-ils conciliables? Pouvons-nous formuler des objectifs et dégager de la valeur de nos investissements dans les TI?
- **Stratégie** – Dans certaines entreprises, les TI constituent un facteur stratégique clé, si bien qu'elles se doivent de rester à la fine pointe de la technologie pour conserver leur avantage concurrentiel. Dans d'autres entreprises, les TI ne représentent plutôt qu'un ensemble de bons outils assurant la prise en charge de leurs activités. Même si les conseils d'administration peuvent considérer les TI davantage comme une source de nouvelles possibilités qu'un secteur de risques d'affaires, l'alignement des TI sur la stratégie de l'entreprise reste un défi important.

[2] Whitehouse, Tammy, *Where IT, Internal Controls Collide, ComplianceWeek*, le 17 octobre 2006. Document accessible à l'adresse suivante : http://www.datablueprint.com/documents/interviews/20061017_whereitinternalcontrolscollide.pdf.

Nécessité pour les conseils d'administration de veiller à une répartition appropriée des responsabilités à l'égard de la surveillance des TI

Les membres du RCCV ont énergiquement débattu de la question à savoir à qui revient la responsabilité des TI au sein du conseil d'administration. Ce dernier assume un rôle de premier plan relativement à certains aspects clés de la gouvernance des TI, particulièrement en ce qui a trait aux systèmes assurant la prise en charge des processus liés à la conformité financière et à la reprise des activités en cas d'urgence (composante des responsabilités du comité de vérification à l'égard de la surveillance des risques), puisque ces processus de reprise ne sont pas visés par l'article 404 de la loi Sarbanes-Oxley. En revanche, les membres du RCCV ont énoncé clairement que le comité de vérification ne devrait pas avoir à assumer l'entière responsabilité à l'égard des aspects de la surveillance des TI se rapportant à l'exploitation et à la stratégie. «Les membres du comité de vérification ne sont pas en mesure de tout assumer seuls; ils ont déjà trop à faire», a fait valoir l'un d'eux.

Nécessité d'intégrer tous les administrateurs aux discussions stratégiques

Les membres du RCCV sont d'avis que, dans les secteurs d'activité où les TI constituent un facteur stratégique, tous les administrateurs devraient s'engager fermement à l'égard de la gouvernance des TI et qu'il revient au comité de vérification d'être le moteur de cet engagement. Ils préviennent toutefois que, même dans les entreprises où les TI représentent un facteur stratégique, la nature de l'engagement du conseil d'administration varie en fonction du secteur d'activité et des incidences liées aux TI.

Les membres du RCCV s'interrogent à savoir s'il est approprié que, dans les entreprises où les TI ne représentent pas un facteur stratégique, le conseil d'administration dans son ensemble s'occupe des questions relatives à la gouvernance des TI. Ils ont tendance à croire que seules les questions se rapportant à d'importantes dépenses en TI devraient alors être portées à l'attention de l'ensemble du conseil d'administration, au même titre que toute dépense importante rattachée à d'autres projets d'immobilisations d'envergure.

Gestion par le comité de vérification des risques de TI liés à l'information financière

Dans le cadre de leurs activités de gouvernance des TI, les comités de vérification se trouvent à appliquer à la fois une approche proactive – en appliquant des mesures préventives – et une approche réactive – en s'efforçant de trouver des solutions aux problèmes qui leur sont soumis.

- **Approche proactive** – Bien des comités de vérification se tournent vers la fonction TI de leur entreprise pour qu'elle leur prête assistance quand vient le temps de régler des problèmes de conformité, mais ils sont toutefois moins nombreux à faire ce qu'il faut pour assurer l'efficacité du plan de reprise en cas d'urgence.
- **Approche réactive** – Les membres du RCCV font remarquer que les comités de vérification héritent des problèmes de TI que les vérificateurs internes ont soulevés dans leur rapport.

Les membres du RCCV s'entendent sur le fait que les défaillances sur le plan de la sécurité et les compromis au chapitre de la protection des renseignements personnels peuvent produire des effets catastrophiques. Les

entreprises doivent non seulement s'occuper des problèmes auxquels elles sont confrontées, mais aussi des incidences qui risquent d'en découler en ce qui a trait à leur réputation. Par ailleurs, les membres du RCCV ont souligné que les problèmes de TI sont rarement, voire jamais, une composante clé des cas de fraude dans les entreprises. «Combien de cas de fraude découlent de déficiences sur le plan des TI?, s'est interrogé ouvertement l'un d'eux. Eh bien, aucun!»

Nécessité pour les conseils d'administration de s'appuyer sur des sources externes et internes spécialisées en TI

Reconnaissant que peu d'administrateurs ont une connaissance approfondie des TI, les membres du RCCV considèrent qu'il est important pour ces derniers de faire appel à des spécialistes capables de les aider à se familiariser suffisamment avec les problèmes pertinents ainsi qu'avec les solutions à y apporter. Ils soulignent qu'il arrive souvent que les vérificateurs externes et les vérificateurs internes communiquent de l'information sur la performance de la fonction TI et sur les problèmes auxquels cette dernière est confrontée.

En outre, les chefs de l'information qui n'ont pas un accès direct à leur comité de vérification souhaiteraient interagir davantage avec celui-ci. Dans une entrevue qu'il a accordée à la publication *InSights*, l'un d'eux a formulé le commentaire que voici : «Bien que le président du comité de vérification soit au fait des problèmes de l'entreprise, cela ne nous ferait pas de mal de nous réunir pour échanger de l'information».[3]

Vérificateurs externes

Les présidents de comités de vérification peuvent discuter des questions relatives aux TI avec les spécialistes en TI du cabinet d'experts-comptables faisant partie de l'équipe de vérification, de façon à s'assurer que les membres de leur comité sont familiers avec l'environnement de TI de l'entreprise ainsi qu'avec les risques et contrôles qui s'y rapportent, de même qu'avec l'ensemble des lacunes constatées sur ce plan. Les membres du RCCV soutiennent que le recours aux compétences de vérificateurs externes présente plusieurs avantages : 1) les vérificateurs externes connaissent bien les activités de l'entreprise ainsi que son organisation; 2) ils savent à quel point les TI influent sur les contrôles et sur les autres secteurs de risque; et 3) les ressources et les compétences qu'ils détiennent leur permettent de faire le point sur les risques, les défis et les possibilités liés aux TI.

Les membres du RCCV soulignent que les vérificateurs externes accompagnent le comité de vérification dans le processus de règlement des questions relatives à la gouvernance des TI, particulièrement en ce qui a trait à l'information financière et à la conformité réglementaire. En revanche, de façon générale, l'examen global de la fonction TI ne fait pas partie de l'étendue des services qui sont rendus dans le cadre d'une mission de vérification.

---

[3] Ernst & Young et Tapestry Networks, *The CIO's perspective*, *InSights*, le 28 février 2005. Volume 7. Document accessible à l'adresse suivante : http://www.tapestrynetworks.com/documents/Tapestry_EY_ACLN_Feb05_InSights.pdf

Vérificateurs internes

Les vérificateurs internes peuvent aider les administrateurs à obtenir une vision plus complète de la fonction TI. L'un des membres du RCCV explique que, en s'appuyant sur des ressources internes appropriées, l'équipe de vérification interne peut dans bien des cas leur donner un nouveau point de vue utile. Néanmoins, malgré le rôle important joué par la vérification interne sur le plan de la gouvernance des TI, les membres du RCCV soulignent qu'il est très difficile pour les entreprises de retenir à leur service des vérificateurs internes compétents. «Les entreprises ont besoin d'une fonction vérification interne des TI, mais elles peuvent difficilement s'en charger elles-mêmes», a fait valoir l'un d'eux. Dans la pratique, il est fréquent que cette fonction soit impartie.

Développement de la relation entre le conseil d'administration et le chef de l'information

Bien que les chefs de l'information jouent un rôle de plus en plus essentiel à l'échelle de l'ensemble des unités fonctionnelles et des fonctions, leur rayonnement au sein des conseils d'administration ne semble pas pour autant gagner en importance. Les administrateurs qui reconnaissent l'importance du chef de l'information et de la fonction TI reconnaissent aussi que les chefs de l'information doivent avoir davantage voix au chapitre au sein des conseils d'administration et des comités de vérification. Les chefs de l'information doivent apporter une contribution accrue et être davantage redevables de leurs actes.

À l'issue de cette réunion du RCCV, l'un des membres du réseau a pris l'engagement d'inscrire le chef de l'information sur la liste des personnes qu'il doit rencontrer plus souvent. Un autre membre a relevé le fait que l'importance accrue des TI au sein de sa propre entreprise est une bonne raison d'amorcer une discussion avec le chef de l'information. Les membres qui ne rencontrent pas déjà régulièrement le chef de l'information de leur entreprise conviennent pourtant avoir grandement besoin de ses compétences, ainsi que des connaissances et du sentiment de confiance qu'ils pourraient acquérir en le côtoyant.

N'est-il pas plus pertinent pour le comité de vérification de se poser les bonnes questions, plutôt que de trouver des solutions toute faites?

Les membres du RCCV sont conscients que des enjeux aussi complexes que ceux touchant la gouvernance des TI suscitent davantage de questions que de réponses. Les administrateurs relèvent la plupart des enjeux, malgré l'incertitude qui les entoure. Les administrateurs doivent donc se demander comment ils peuvent s'acquitter de leurs responsabilités à l'égard de la gouvernance de leur entreprise sans risquer de transgresser la fine ligne de démarcation qui existe entre la fonction Surveillance et la fonction Gestion.

D'après une étude réalisée par Burson-Marsteller, en 2004, seulement 8 % des conseils d'administration des 500 sociétés du palmarès *Fortune Global* comptaient ou avaient compté en leurs rangs un chef de l'information.[4] Les membres du RCCV ne s'entendent pas sur la question à savoir s'il est important que les comités de vérification comptent des membres compétents dans le domaine des TI. Dans une entrevue

[4] Burson-Marsteller, A Missing Competency: *Boardroom IT-deficit* (Burson-Marsteller, 2005), 4. Document accessible à l'adresse suivante : http://www.burson-marsteller.com/pdf/IT_Deficit_2005_Brochure.pdf

accordée avant la plus récente réunion du RCCV, l'un d'eux a prévenu que l'intégration au comité de vérification d'un soi-disant spécialiste des TI ne permettrait pas nécessairement d'obtenir l'expérience requise sur le plan de la surveillance des TI : «Je fais partie d'un conseil d'administration auquel siège également un haut responsable des TI et, franchement, je dois dire qu'il ne se signale pas particulièrement par sa contribution à l'égard de la surveillance des TI et qu'il ne s'y connaît guère plus que les autres administrateurs. Il n'est pas capable d'analyser en profondeur les questions à régler.» D'autres membres croient cependant que les administrateurs qui exercent ou qui ont déjà exercé des fonctions de responsable des TI peuvent être une source importante de valeur. «Le conseil d'administration doit surmonter le défi que représente la nécessité de s'assurer de la compétence des responsables, souligne l'un d'eux. Les comités de vérification qui comptent en leurs rangs des spécialistes des TI sont en mesure d'appliquer une approche plus pragmatique.»

Prochaines étapes et mesures immédiates préconisées par les membres du RCCV

- *Interagir davantage avec le chef de l'information* – Les membres croient que les comités de vérification gagneraient à interagir davantage avec le chef de l'information de leur entreprise, dans le cadre d'échanges aussi bien officiels qu'officieux.
- *Faire appel aux ressources appropriées* – Les vérificateurs externes, les vérificateurs internes et les cabinets d'experts-conseils en TI peuvent aider les administrateurs à se familiariser avec les pratiques et enjeux en matière de gouvernance des TI.
- *Améliorer la gouvernance des TI* – Les membres soutiennent que les conseils d'administration doivent s'engager dans une analyse plus globale favorisant une meilleure compréhension des risques de TI ainsi qu'une répartition plus efficace des responsabilités à cet égard.
- *Intégrer les compétences en TI au cadre de compétences du conseil d'administration* – Certains membres considèrent que les entreprises devraient envisager la possibilité d'intégrer les compétences en TI à leur cadre de compétences, au même titre que les compétences en finances ayant été intégrées à la suite de l'entrée en vigueur de la loi Sarbanes-Oxley.

Conclusion

Dans un monde caractérisé par l'omniprésence des TI, les entreprises font face aux nouvelles possibilités et aux nouveaux risques qui en découlent. Des communications claires et des relations solides doivent prévaloir, de façon à favoriser l'élimination des chevauchements en matière de gouvernance et à faire en sorte qu'aucun aspect ne soit escamoté.

Bien que peu d'administrateurs considèrent être des spécialistes des TI, ils peuvent faire appel à diverses sources de compétences afin d'orienter leurs démarches. De plus, en commençant par reconnaître qu'ils ont parfois plus de questions à poser que de solutions à proposer, les présidents de comités de vérification finiront par se sentir davantage en mesure de traiter des questions relatives aux TI, de la même façon qu'ils en sont venus à se familiariser avec d'autres questions sur lesquelles les comités de vérification ont maintenant plus l'habitude de se pencher.

Les points de vue exprimés dans le présent document vont dans le même sens que ceux que défend le Réseau canadien des comités de vérification (RCCV), dont les membres exercent des fonctions de président de comité de vérification au sein de grandes sociétés canadiennes et se sont engagés à améliorer le rendement de leur comité de vérification et à promouvoir la confiance envers les marchés de capitaux. Ils ne coïncident pas nécessairement avec l'opinion individuelle des membres du réseau, ni avec le point de vue de leur société, d'Ernst & Young ou de Tapestry Networks. Pour obtenir un avis particulier, veuillez consulter vos conseillers. Ernst & Young désigne l'ensemble des membres d'Ernst & Young Global.

Annexe : Questions à considérer par les conseils d'administration dans le cadre de la poursuite de leurs objectifs en matière de gouvernance des TI[5]

Évaluation de l'alignement entre les activités organisationnelles et les objectifs en matière de TI

Objectifs

Amener les entreprises et leur fonction TI à s'entendre sur une définition commune du rôle des TI et sur la contribution des entreprises en la matière, de même qu'à bien comprendre ce rôle et cette contribution. Faire en sorte que les hauts responsables des TI et les membres de la haute direction des entreprises s'engagent dans la gouvernance des TI, qu'ils soient redevables à cet égard et qu'ils soutiennent le conseil d'administration dans l'établissement des orientations à suivre.

Questions clés à poser

- Les administrateurs de votre entreprise sont-ils clairement tenus de rendre des comptes relativement aux questions touchant les TI?
- Quel type de formation les administrateurs de votre entreprise reçoivent-ils de façon à favoriser l'efficacité des discussions axées sur les TI et à leur permettre d'acquérir davantage d'assurance en la matière? Dans quelle mesure ont-ils l'assurance nécessaire pour engager de telles discussions et y contribuer?
- Les administrateurs de votre entreprise comprennent-ils les dépenses de TI effectuées par celle-ci ainsi que le lien entre ces dépenses et la stratégie et les objectifs organisationnels? Dans quelle mesure existe-t-il une compréhension commune de ce que peut représenter la valeur des TI?
- Les administrateurs de votre entreprise arrivent-ils à s'entendre sur la définition d'un ensemble d'équipements de TI essentiels et des risques qui s'y rapportent? Les zones d'interdépendance entre les TI et les risques d'entreprise sont-elles clairement définies? Dans quelle mesure avez-vous l'assurance qu'une approche harmonisée des risques peut être mise en œuvre à l'échelle organisationnelle?

Dégager de la valeur grâce à la surveillance de la gestion des investissements en matière de TI

Objectifs

Faire preuve de rigueur sur le plan de la gouvernance dans le cadre de l'évaluation des nouvelles initiatives proposées, de l'établissement de leur priorité et de la surveillance des progrès accomplis. Assurer le maintien de la cohérence des buts et objectifs associés aux projets et veiller à la réalisation des avantages escomptés, et

[5] Questions formulées par Ernst & Young à la suite de la réunion du RCCV tenue le 3 avril 2007 et destinées à servir de référence pour les comités de vérification et les administrateurs.

ce, sans entraver l'évolution des besoins de l'entreprise et les modifications à apporter à la gestion des risques d'affaires, une telle évolution et de telles modifications étant inévitables au cours de programmes de longue durée. Se familiariser avec les inducteurs de coûts de TI et les enjeux en la matière, avec l'envergure et la nature des budgets et des dépenses de TI, de même qu'avec le cadre de surveillance de ces dépenses.

Questions clés à poser

- Le conseil d'administration, les responsables des TI et la fonction Finances s'entendent-ils sur la répartition, l'évaluation et la surveillance des coûts et de la valeur liés aux TI?
- Comment obtient-on l'aval des intéressés tout en les rendant redevables relativement aux nouveaux investissements dans les systèmes et aux avantages devant en découler?
- Une méthode d'évaluation en bonne et due forme des portefeuilles est-elle appliquée aux nouveaux projets envisagés? S'agit-il d'une méthode cohérente, bien assimilée et répondant à la nécessité de disposer de critères d'évaluation multiples adaptés à un programme particulier?

Respect des exigences de conformité

Objectifs

Mettre en œuvre un cadre de travail et un processus permettant d'assurer le recensement efficace et efficient des exigences de conformité et leur respect. Acquérir l'assurance que les TI sont soumises à des contrôles adéquats, de façon à favoriser l'assimilation et le respect de la multitude d'exigences de conformité s'appliquant aux TI.

Questions clés à poser

- Avez-vous l'assurance de vraiment bien comprendre les incidences de programmes de conformité tributaires des TI, tels que ceux se rapportant à l'article 404 de la loi Sarbanes Oxley, au Règlement 52-109, aux normes IFRS et à la huitième directive de l'Union européenne?
- Dans votre entreprise, des conseillers internes et des conseillers externes évaluent-ils les TI afin d'assurer leur conformité aux exigences réglementaires et font-ils rapport au conseil d'administration à cet égard?
- Une méthode rigoureuse est-elle appliquée à l'échelle de l'entreprise afin d'assurer la prise en compte des nouvelles exigences de conformité ainsi que le respect des exigences de base, à tout le moins?
- Les responsabilités à l'égard de l'atteinte des objectifs de conformité et du maintien de la conformité sont-elles clairement définies? Le conseil d'administration est-il régulièrement informé des résultats obtenus sur ce plan?
- Une fois que les mesures initiales axées sur la conformité aux exigences réglementaires ont été mises en œuvre, comment l'entreprise fait-elle pour en assurer l'intégration à ses façons de faire?

Évaluation de la performance

Objectifs

Accroître la probabilité que la fonction TI puisse combler l'écart entre sa performance perçue et sa performance réelle, puis en tenir compte dans sa contribution à l'entreprise. Acquérir l'assurance de prendre des décisions judicieuses sur le plan des investissements en s'appuyant sur l'accessibilité à de l'information exacte et pertinente. Faire en sorte que l'ensemble des parties prenantes s'entendent sur les aspects importants et établissent un cadre de travail favorisant le rajustement des mesures au fur et à mesure que l'entreprise évolue et que ses critères d'évaluation du succès changent.

Questions clés à poser

- Votre entreprise a-t-elle réussi à établir un consensus autour d'une vision correspondant à une bonne performance des TI? Dispose-t-elle de mesures discrètes pour ses importants investissements stratégiques dans le secteur des TI?
- Comment votre entreprise a-t-elle déterminé les aspects à évaluer? S'est-elle assurée de disposer des outils et processus d'évaluation nécessaires? Reçoit-elle des rapports sur les résultats de cette évaluation?
- Quelles mesures ont été mises en œuvre consécutivement à l'évaluation de la performance des TI?
- Le processus d'évaluation des TI fait-il partie intégrante du processus d'évaluation de la performance de l'entreprise, et ces processus sont-ils exécutés concurremment?
- Votre cadre d'évaluation est-il adaptable en fonction de la modification des priorités de l'entreprise et, par conséquent, en fonction de la modification des mesures de la performance des TI?

Élaboration et mise en œuvre d'un cadre de gestion des risques cohérent

Objectifs

Mettre en œuvre des moyens bien en vue permettant de faire valoir ses préoccupations et de signaler les problèmes constatés en matière de TI. Acquérir l'assurance que les programmes sont en voie de produire des rapports précis sur les risques. Appliquer des critères clairs permettant d'orienter les décisions aux étapes essentielles des programmes et le soutien au changement ou encore d'interrompre rapidement les programmes voués à l'échec.

Questions clés à poser

- Existe-il à l'échelle de l'entreprise une méthode claire de gestion des risques? Cette méthode est-elle appliquée aux TI?
- À votre connaissance, à quand remonte la plus récente évaluation globale des risques de TI au sein de votre entreprise? Les résultats de cette évaluation ont-ils fait l'objet d'une vérification indépendante?

- Dans quelle mesure avez-vous l'assurance que l'évaluation et la gestion des risques font véritablement partie des compétences de base à l'échelle organisationnelle?
- Dans quelle mesure avez-vous l'assurance que les risques de TI sont classifiés suivant une approche rigoureuse? Une fois que cette classification est effectuée, s'occupe-t-on seulement des risques élevés?
- Comment votre entreprise mesure-t-elle l'efficacité de ses stratégies et activités de gestion des risques?
- La gestion des risques est-elle véritablement intégrée à l'échelle organisationnelle, ou considère-t-on qu'elle relève plutôt des vérificateurs et des responsables de la conformité?

Efficacité de la fonction TI et de la gestion des ressources

Objectifs

Procéder régulièrement à une évaluation en bonne et due forme de la fonction TI, de façon à dégager de la valeur des dépenses en TI (sur le plan des ressources humaines, technologiques et financières) et à faire les bons choix en ce qui a trait aux coûts et aux risques dans le cadre des stratégies d'approvisionnement des TI et de la prise des décisions en la matière. Acquérir l'assurance que la fonction TI est rentable, que les coûts associés aux systèmes qu'elle a mis en œuvre sont comparables à ceux auxquels font face les chefs de file du secteur, que le personnel affecté aux TI est compétent et bien formé et que l'équilibrage des ressources en la matière est efficace. Mettre en œuvre une structure pouvant être évaluée sur le plan des ressources, du recrutement, de la rémunération et des avantages sociaux. Comprendre les premiers signes avertisseurs d'un décalage éventuel entre la capacité sur le plan des TI et les objectifs d'affaires visés. Conserver la latitude nécessaire en ce qui a trait à la gestion des ententes d'impartition.

Questions clés à poser

- De quelle façon la fonction TI de votre entreprise est-elle alignée sur sa stratégie?
- À quand remonte la dernière fois où la fonction TI de votre entreprise a dû justifier l'importance de son effectif et l'équilibrage de ses compétences?
- À quand remonte la plus récente évaluation rigoureuse des capacités organisationnelles de la fonction TI de votre entreprise?
- Dans quelle mesure les capacités organisationnelles de la fonction TI influent-elles sur les décisions relatives à l'approvisionnement?
- Comment justifiez-vous le budget que votre entreprise consacre à la formation en TI? Ce budget est-il aligné sur sa stratégie en matière de TI?
- Avec quelle facilité les décisions en matière d'approvisionnement peuvent-elles être renversées ou modifiées après leur adoption? Et à quel prix cela est-il possible?

Assurer l'application par les tiers de pratiques de gouvernance efficaces

Objectifs

S'entendre dès le départ sur une définition claire des objectifs visés et des normes à suivre, et en tenir compte dans l'élaboration de contrats en bonne et due forme alignés sur les exigences particulières. Mettre en place un cadre de gouvernance adapté à l'ensemble du cycle d'impartition. Assurer un contrôle préalable complet et définir les indicateurs de rendement clés avant la signature des contrats.

Questions clés à poser

- Les intéressés clés s'entendent-ils sur les objectifs principaux et secondaires à atteindre dans le cadre de la collaboration avec des tiers? S'agit-il d'accroître l'efficacité, de réduire les coûts, d'améliorer l'accès aux compétences ou de soutenir le passage d'une étape à une autre au sein de votre entreprise?
- Sur le plan de la culture, votre entreprise et le tiers potentiel sont-ils compatibles? Les valeurs du tiers s'apparentent-elles à celles de votre entreprise?
- Les critères et mécanismes d'évaluation du succès sont-ils clairement définis?
- Dans quelle mesure avez-vous l'assurance de détenir les compétences nécessaires pour gérer efficacement la relation avec le tiers?
- Les responsabilités et les exigences en matière de reddition de comptes sont-elles clairement définies, consignées et comprises par votre entreprise et par le tiers?
- Les fournisseurs tiers sont-ils à la hauteur de vos exigences en ce qui a trait à la conformité aux principales mesures de la conformité / des risques prévues à l'entente?