

20 Questions

que les administrateurs devraient poser sur
les technologies de l'information

Révision : avril 2004



Comment utiliser le présent cahier

Chaque cahier de la série «20 Questions» se veut une introduction concise et accessible à un sujet d'intérêt pour les administrateurs. L'utilisation de questions tient compte du rôle de surveillance des administrateurs, qui comprend le fait de poser à la direction — et de se poser à eux-mêmes — des questions pénétrantes. L'ensemble des questions ne constitue pas une «liste de contrôle» exhaustive, mais bien un moyen de fournir un éclairage et de stimuler les discussions sur des sujets importants.

Les commentaires qui accompagnent les questions résument les considérations actuelles sur les problèmes d'organisations prééminentes et fournissent aux administrateurs des assises pour évaluer de façon éclairée les réponses qu'ils obtiennent et pour approfondir le questionnement au besoin. Bien que les questions s'appliquent à la plupart des organisations de moyenne et de grande taille, les réponses varieront selon la taille, la complexité et le degré d'évolution de chaque organisation.

Comité consultatif sur les technologies de l'information de l'ICCA

20 Questions

que les administrateurs devraient poser sur
les technologies de l'information

Révision : avril 2004

Catalogage avant publication de Bibliothèque et Archives Canada

20 questions que les administrateurs devraient poser sur les technologies de l'information. — Révision, avril 2004.

(Collection Gestion des risques et gouvernance)

Traduction de: 20 questions directors should ask about IT.

Comprend des réf. bibliogr.

ISBN 1-55385-123-4

1. Technologie de l'information — Gestion. 2. Systèmes d'information de gestion. 3. Administrateurs de sociétés. I. Institut canadien des comptables agréés. II. Titre: Vingt questions que les administrateurs devraient poser sur les technologies de l'information. III. Collection.

HD30.2.T8814 2004

658.4'038

C2004-904851-1

Tous droits réservés © 2004

L'Institut Canadien des Comptables Agréés

277, rue Wellington Ouest

Toronto (Ontario) M5V 3H2

Imprimé au Canada

Available in English

Préface

Le Comité consultatif sur les technologies de l'information de l'ICCA a préparé la présente brochure pour aider les membres des conseils d'administration à étudier les questions de technologies de l'information (TI) qui peuvent surgir dans le cadre de l'exercice de leurs fonctions. Ce document pourrait également présenter un intérêt et être utile pour les membres d'autres instances de gouvernance, en particulier les comités de vérification, et les membres d'organismes stratégiques tels que les comités d'orientation sur les TI.

On attend des administrateurs d'organisations qu'ils s'assurent que la fonction des TI soit efficace. Le présent document contient des exemples de questions que les conseils d'administration peuvent poser au chef des TI et à d'autres personnes. Chaque question est accompagnée de brèves explications contextuelles. Nous espérons que les administrateurs, les chefs de la direction et les chefs de l'information trouveront ce document utile pour évaluer leur approche à l'égard de la gestion des risques et du contrôle interne.

L'ICCA tient à exprimer sa plus vive reconnaissance aux membres du Comité consultatif sur les technologies de l'information pour la production de la présente brochure.

Comité consultatif sur les technologies de l'information de l'ICCA

Président

Donald E. Sheehy, CA•CISA, Deloitte & Touche LLP, Toronto

Comité

Gary S. Baker, CA, Deloitte & Touche LLP, Toronto

David Chan, CA•CISA, Centre de protection de l'information, gouvernement de l'Ontario, Toronto

Allan W.K. Cheung, CA•TI, CISA, La Caisse canadienne de dépôt de valeurs limitée, Toronto

Henry Grunberg, CA•TI, Ernst & Young LLP, Toronto

Ray Henrickson, CA•TI/CISA, La Banque Scotia, Toronto

Carole Le Néal, CISA, Mouvement des caisses Desjardins, Montréal

James R. Murray, CA, CISA, Grant Thornton LLP, Halifax

Erlinda L. Olalia-Carin, CISA, KPMG LLP, Toronto

Robert G. Parker, FCA, CA•CISA, Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•CISA, PricewaterhouseCoopers LLP, Winnipeg

Douglas G. Timmins, CA, Bureau du vérificateur général du Canada, Ottawa

Gerald D. Trites, FCA, CA•CISA, St. Francis Xavier University, Antigonish (Nouvelle-Écosse)

(consultant contractuel affecté au Comité)

Bryan C. Walker, CA, L'Institut Canadien des Comptables Agréés, Toronto

Personnel de l'ICCA

William J.L. Swirsky, FCA, vice-président, Développement des connaissances

Andrée Lavigne, CA, directrice de projets, Monographies

Responsabilités du conseil à l'égard des technologies de l'information

Le conseil d'administration voit à l'orientation stratégique et à la gestion générale de l'organisation. À ce titre, il doit se tenir au courant des questions relatives aux systèmes de gestion et de contrôle mis en place pour maintenir à un niveau acceptable le risque de perte découlant des fraudes et des erreurs. En outre, en janvier 2004, les Autorités canadiennes en valeurs mobilières (ACVM) ont adopté de nouveaux règlements¹ visant à rétablir la confiance des investisseurs. Ceux-ci comprennent des exigences semblables à celles découlant de la Loi Sarbanes-Oxley aux États-Unis et établissent de nouvelles responsabilités importantes à l'égard du contrôle interne. Du point de vue des technologies de l'information (TI), le Règlement 52-109 présente un intérêt particulier puisqu'il prévoit que le chef de la direction et le chef des finances seront tenus d'attester, entre autres :

- qu'ils ont mis en place des contrôles internes et des contrôles et procédures de communication de l'information financière (ou ont pris des mesures pour qu'ils soient conçus sous leur supervision);
- qu'ils ont évalué l'efficacité de ces contrôles et procédures de communication de l'information et ont pris des mesures pour que ceux qui émettent ces contrôles et procédures communiquent leurs conclusions concernant cette évaluation;
- qu'ils ont pris des mesures pour que ceux qui émettent les contrôles et procédures communiquent certains changements concernant le contrôle interne à l'égard de l'information financière.

Par déduction, il incombe aux membres du conseil de surveiller les systèmes de contrôle et de poser les bonnes questions pour s'assurer qu'ils ont été conçus adéquatement et qu'ils fonctionnent correctement

et que des processus ont été mis en place afin de garantir que les obligations juridiques de la direction sont remplies.

Les TI jouent depuis plusieurs années un rôle important dans les systèmes de gestion et de stratégie organisationnelle. Pour les généralistes que sont la plupart des administrateurs, cependant, il est souvent difficile de suivre l'évolution rapide des TI et, par conséquent, de savoir quelles questions poser pour s'assurer que les problèmes dans ce domaine sont adéquatement pris en compte.

Selon les lignes directrices en matière de régie d'entreprise de la Bourse de Toronto (article 474), les responsabilités du conseil d'administration sont les suivantes :

«Le conseil d'administration doit assumer explicitement la responsabilité de gérance de l'entreprise et, dans le cadre de la responsabilité générale de gérance, il doit assumer la responsabilité des questions suivantes :

- l'adoption d'un processus de planification stratégique;
- l'identification des principaux risques associés aux activités de l'entreprise et la prise de mesures assurant la mise en œuvre de systèmes appropriés permettant la gestion de ces risques;
- la planification de la relève, y compris la nomination, la formation et la supervision des hauts dirigeants;
- la politique de communication de l'entreprise;
- l'intégrité des systèmes de contrôle interne et d'information de gestion de l'entreprise.»

¹ Les règlements visant à rétablir la confiance des investisseurs incluent le Règlement 52-108 sur la surveillance des vérificateurs, le Règlement 52-109 sur l'attestation de l'information présentée dans les documents annuels et intermédiaires des émetteurs et le Règlement 52-110 sur les comités de vérification.

Comme cette liste l'indique, le maintien de l'intégrité des systèmes de contrôle interne et d'information de gestion compte parmi les responsabilités importantes du conseil. Cette responsabilité est liée étroitement à celle de l'identification et de l'évaluation des risques du fait que les systèmes de contrôle interne sont généralement fondés sur le risque. Le processus de planification stratégique, dont fait partie le suivi de la performance, est un élément important du système de contrôle.

La présente brochure propose les questions que les membres du conseil devraient poser pour s'acquitter des responsabilités ci-dessus. Ces questions sont regroupées selon les trois grands champs : stratégie, contrôle interne et risques.



Questions relatives à la stratégie

I Stratégie et planification

Volet important de la stratégie, le processus de planification stratégique doit être appliqué au secteur des systèmes d'information (SI) en conformité avec la politique globale de l'entreprise en la matière. La planification stratégique pour les SI peut être intégrée au processus général de planification pour l'ensemble de l'entreprise ou constituer une activité distincte étroitement liée à la planification générale. Tous les éléments habituels de la planification stratégique de l'entreprise doivent se retrouver dans celle des SI, à savoir la participation et le soutien de la haute direction, la participation des employés clés et l'intégration de plans d'action. Ces plans sont habituellement incorporés au plan tactique. Élaboré tous les ans, le plan tactique découle du plan stratégique, mais il prévoit le suivi, la mise à jour et la révision périodiques des budgets, des ressources, des niveaux de compétence, de l'information sur les projets, des partenaires clés, etc.

La principale question à poser concernant la planification stratégique est la suivante :

1. **La direction a-t-elle un plan stratégique en matière de systèmes d'information qu'elle surveille et met à jour selon les besoins? Ce plan sert-il de base aux plans annuels, aux budgets annuels et à long terme, et à la priorisation des projets en technologies de l'information?**

II Tendances technologiques

Pour que les systèmes d'information d'une organisation demeurent à jour, celle-ci doit suivre de près les tendances de la technologie. C'est encore plus vrai à l'heure des affaires électroniques et de l'intégration accrue avec les partenaires commerciaux, les clients et les fournisseurs. Les organisations qui continuent d'utiliser des systèmes anciens ou désuets risquent d'avoir de la difficulté à les intégrer aux systèmes plus récents, et ainsi rater des occasions intéressantes. D'où l'importance de se tenir au courant des tendances technologiques et d'envisager régulièrement de mettre à niveau le matériel et les logiciels dans un contexte de rendement du capital investi. L'organisation répartit ainsi les coûts sur plusieurs années au lieu d'investir massivement dans le remplacement de gros modules désuets.

La question à poser est la suivante :

2. **L'organisation a-t-elle mis en place des procédures appropriées pour se tenir au courant des tendances technologiques, pour les évaluer périodiquement et pour en tenir compte dans sa stratégie de positionnement?**

III Performance

L'information sur la performance organisationnelle est indispensable à toute activité de planification stratégique du fait qu'elle permet de cibler les éléments qui, une fois améliorés ou modifiés, seront rentables et efficaces. Les activités de suivi qui produisent cette information reposent sur la sélection des mesures de performance appropriées et la mise au point de systèmes pour informer le personnel de direction clé.

Deux questions devraient être posées :

- 3. Les indicateurs et inducteurs de performance clés du service des TI ont-ils été établis? En fait-on régulièrement le suivi et les compare-t-on aux normes du secteur?**
- 4. Les indicateurs pertinents ont-ils été établis et en fait-on le suivi pour assurer la gestion de la performance des tiers fournisseurs de services de l'organisation?**

IV Personnel

Embaucher des employés suffisamment compétents et les retenir représente un défi à l'ère de l'information. Sans eux, les systèmes de TI ne peuvent fonctionner efficacement.

Pour recruter et retenir de tels employés, l'organisation doit pouvoir compter sur des programmes solides qui lui permettent de contrôler le roulement de personnel, d'orienter la formation et de favoriser le perfectionnement professionnel. C'est le conseil d'administration qui assume l'ultime responsabilité de la mise en place de ces programmes et de leur efficacité.

On posera à cet égard deux questions clés :

- 5. Comment la direction a-t-elle déterminé l'expertise technologique nécessaire et quels moyens utilise-t-elle pour attirer les employés les plus talentueux?**
- 6. La direction a-t-elle mis en place des procédures appropriées en matière de roulement, de formation et d'affectation des employés du service des technologies de l'information?**

V Gouvernance

Il existe plusieurs façons de structurer la gouvernance en ce qui concerne les TI; le choix d'un modèle en particulier repose sur des facteurs tels que la nature de l'organisation, sa structure de gestion, sa culture et l'importance relative des TI au regard des objectifs stratégiques généraux.

Certains principes valent pour la plupart des organisations. Il doit y avoir un lien direct entre la gestion des TI et les plus hauts niveaux de direction de l'organisation. Bon nombre d'entreprises nomment un chef de l'information, qui relève directement du chef de la direction, du comité de vérification et, souvent, du conseil. Il arrive parfois que la personne responsable des TI soit chargée d'autres fonctions à un niveau de direction, lesquelles peuvent être aussi étendues, sinon plus. Ce n'est généralement pas une bonne idée, comme cela s'est souvent produit dans le passé, de confier la responsabilité des TI à un cadre supérieur du service des finances; les questions financières prennent alors souvent une importance trop grande au détriment d'autres fonctions plus stratégiques ou opérationnelles.

La nécessité de faire participer le personnel à la formulation des stratégies et à la mise en œuvre des politiques est un autre principe essentiel d'une gouvernance efficace dans ce secteur. Le personnel joue ainsi un rôle utile dans le processus de planification stratégique. Il se montrera efficace dans la mise en œuvre des politiques dans la mesure où il les connaît bien et où il y souscrit. La communication claire des politiques est cependant un élément fondamental de leur mise en œuvre.

Un des membres du conseil doit être expressément chargé d'assurer la liaison avec le responsable des TI, et de tenir des rencontres périodiques sur les stratégies, les politiques et la performance.

Pour remplir son mandat de gouvernance en ce qui concerne les TI et afin d'obtenir une assurance quant à la conformité à la Loi Sarbanes-Oxley et aux règlements des ACVM visant à rétablir la confiance des investisseurs, le conseil devrait étudier les questions suivantes :

- 7. Le conseil a-t-il envisagé la création d'un sous-comité des TI ou a-t-il confié à l'un ou plusieurs de ses membres la responsabilité des investissements de l'organisation dans les TI et de leur utilisation?**
- 8. La responsabilité de la gouvernance en matière de TI incombe-t-elle à une personne occupant un poste de direction suffisamment élevé? Comment la direction communique-t-elle les politiques de l'organisation en matière de TI aux employés?**
- 9. Quelles sont les procédures mises en place pour assurer que les systèmes et la gestion de l'entreprise soient conformes aux exigences de la Loi Sarbanes-Oxley et/ou des règlements des ACVM visant à rétablir la confiance des investisseurs, le cas échéant?**

VI Risques et contrôles

Le lien entre le risque et les contrôles est évident. Dans un environnement de TI, le risque s'entend de la probabilité qu'une erreur ou une interruption de traitement survienne dans un système donné et que cette erreur ou interruption ait une incidence sur l'exploitation de l'organisation. L'organisation doit d'abord analyser les événements et les circonstances qui menacent les systèmes d'information et déterminer le degré de risque. S'il est rare qu'on puisse éliminer le risque, les contrôles peuvent permettre de le réduire à un niveau acceptable. Une analyse avantages-coûts convient très bien dans ce contexte. Le niveau de risque acceptable déterminé permettra de définir le type et le niveau de contrôles requis et donc d'établir les ressources qui seront affectées aux contrôles.

Cette démarche repose au départ sur une stratégie très claire de gestion des risques portant sur les menaces qui pèsent sur le système, l'analyse des risques, et la mise en œuvre et la surveillance des contrôles. Les organisations élaborent parfois des plans stratégiques distincts en matière de sécurité qui concordent avec les plans stratégiques établis pour l'ensemble de l'organisation et pour le secteur des TI. Une telle initiative est louable.

L'un des éléments essentiels de ce processus est une structure de suivi efficace, qui permet de passer en revue régulièrement les analyses de risque et le caractère adéquat des mesures de contrôle en vigueur. Cette structure est intégrée formellement à l'organisation et relève ultimement de la personne responsable des TI.

On doit poser trois questions dans le contexte du risque et du contrôle :

10. **La direction planifie-t-elle des évaluations périodiques des risques liés à l'utilisation des technologies de l'information par l'organisation, et notamment aux systèmes et processus internes, à l'externalisation de services et au recours à des services de communications indépendants et à d'autres services? Le cas échéant, prend-elle les mesures appropriées ou nécessaires compte tenu des résultats de ces évaluations?**
11. **Comment la direction assure-t-elle l'intégrité des données et, par le fait même, leur pertinence, leur intégralité, leur exactitude, la rapidité de leur diffusion et leur utilisation judicieuse au sein de l'organisation?**
12. **Quelles dispositions ont été prises par l'organisation pour qu'aient lieu l'examen et la vérification périodiques de ses systèmes, afin d'assurer que les risques soient suffisamment atténués et que ses processus clés soient appuyés par des contrôles?**

VII Protection des renseignements personnels

La protection des renseignements personnels est une priorité du monde des affaires qui requiert une attention constante. Par suite de l'adoption, aux paliers fédéral et provincial, de nouvelles lois sur la protection des renseignements personnels, de nouvelles règles, souvent très strictes, régissent maintenant la propriété des données et les mesures que les organisations en possession de renseignements personnels doivent mettre en œuvre pour protéger la vie privée. Ces lois, ainsi que d'autres lois semblables ailleurs dans le monde, donnent un nouveau sens à la protection des renseignements personnels et obligent les entreprises à assumer des responsabilités plus grandes.

Beaucoup d'organisations ont réagi à la nouvelle donne en établissant des politiques expressément centrées sur la protection des renseignements personnels. Certaines ont chargé des membres de leur personnel d'élaborer et de communiquer des politiques en matière de protection des renseignements personnels et de prescriptions législatives, de surveiller le respect de ces politiques et d'agir en tant que personne-ressource sur ces questions auprès de leurs collègues. Il va de soi que ces personnes jouent un rôle important au sein de l'équipe de direction en veillant à ce que l'aspect protection des renseignements personnels soit pris en compte dans toutes les nouvelles initiatives.

Les questions que l'on doit poser sont les suivantes :

- 13. L'organisation a-t-elle nommé un responsable des politiques en matière de protection des renseignements personnels, des lois en la matière et du respect de celles-ci?**
- 14. L'organisation a-t-elle identifié les diverses exigences contenues dans les textes législatifs et réglementaires quant à la protection des renseignements personnels et a-t-elle élaboré une politique et des procédures pour assurer leur respect?**

VIII Affaires électroniques

Lorsqu'une organisation se lance dans les affaires électroniques, elle s'expose non seulement à de nouveaux risques, mais voit les risques déjà présents accentués par le recours à Internet et par les nombreuses menaces émanant du Web.

La menace d'une intrusion par l'entremise d'Internet ou d'un réseau privé très étendu nécessite l'implantation de contrôles plus rigoureux, comme l'installation de pare-feu, de systèmes de détection des intrus, de systèmes améliorés d'identification des utilisateurs et de mots de passe, ainsi que l'élaboration de politiques destinées à resserrer le contrôle des accès à un niveau proportionnel à ce risque considérable. Le niveau de risque circonstanciel doit être examiné et évalué à fond. Le risque est influencé par la nature de l'entreprise, son profil, la composition de sa clientèle et les méthodes de paiement utilisées.

Voici deux questions pertinentes à poser :

15. **Si l'organisation fait appel aux affaires électroniques pour acheter ou vendre des produits ou des services, a-t-elle fait faire un examen particulier des risques et des contrôles relatifs aux affaires électroniques?**
16. **Les activités d'affaires électroniques de l'organisation sont-elles suffisamment protégées contre une attaque externe ou interne par des personnes non autorisées ou d'autres personnes qui, en cas de réussite, se traduirait par une baisse de la satisfaction de ses clients ou porterait atteinte à son image publique?**

IX Disponibilité

La plupart des entreprises étant aujourd'hui très dépendantes de leurs systèmes d'information, elles voient leur productivité diminuer lorsque ces systèmes tombent en panne, car une partie ou la totalité de leur personnel est alors incapable de faire leur travail. On doit absolument mettre en place des plans qui garantissent que les systèmes seront entièrement opérationnels le plus tôt possible après une interruption de service. Pour assurer la disponibilité des systèmes d'information, on doit élaborer des plans de reprise systématiques qui sont testés et prêts à être déployés en tout temps.

Comme c'est le cas pour toutes les questions de contrôle, on doit tenir compte du degré de risque lorsque l'on détermine l'étendue des contrôles à utiliser. Un système centralisé, par exemple, est généralement exposé à un risque plus grand qu'un système décentralisé, où le risque peut être mieux réparti. Même dans ce dernier cas, on doit toujours avoir des plans permettant, en cas de défaillance d'un élément du système, de recourir à la capacité d'autres éléments. L'importance des périodes d'interruption de service éprouvées par l'organisation par le passé est un bon indice du degré de risque.

Dans ce contexte, les administrateurs doivent poser les questions suivantes :

- 17. L'organisation a-t-elle adopté des politiques officielles relatives à la disponibilité? A-t-elle mis en œuvre des contrôles efficaces destinés à procurer une assurance raisonnable que les systèmes et les données sont disponibles en conformité avec ces politiques?**
- 18. L'organisation comprend-elle l'incidence d'une interruption de service et a-t-elle mis en place des plans pour gérer les interruptions potentielles? A-t-elle adopté un plan de continuité de l'exploitation? Le cas échéant, ce plan fait-il l'objet de tests périodiques et l'améliore-t-on à la lumière des résultats?**

X Aspects juridiques

La question de la conformité aux permis d'utilisation de logiciels a soulevé un certain nombre de problèmes d'ordre juridique, en raison surtout de la reproduction illégale des logiciels et de l'emploi de copies dans les systèmes d'entreprise. La propriété intellectuelle fait de plus en plus l'objet de procédures judiciaires et certaines organisations ont été obligées de payer d'énormes amendes. Lorsque ces questions ont une incidence significative sur l'organisation, l'ultime responsabilité en incombe au conseil.

La direction doit mettre en œuvre des programmes en vue d'atténuer le risque d'infraction à la loi dans ce domaine. Elle doit livrer un message sans équivoque et chercher à convaincre le personnel que l'utilisation de logiciels non autorisés ou reproduits illégalement ou d'autres infractions liées aux données sont inacceptables. Beaucoup d'entreprises prennent des précautions telles que des vérifications logicielles annuelles, l'instauration de politiques sur l'approvisionnement et l'examen périodique des ententes juridiques afin d'établir que toutes les procédures nécessaires au respect des obligations légales sont en place. Ces questions peuvent également être traitées par l'instauration de politiques visant à s'assurer que les systèmes d'information sont utilisés à des fins acceptables pour l'organisation.

Les administrateurs doivent poser les questions suivantes :

- 19. La direction a-t-elle pris en considération et analysé les incidences juridiques relatives à l'utilisation des logiciels et du matériel, aux ententes de service et aux lois sur le droit d'auteur?**
- 20. A-t-on formulé des politiques sur les permis d'utilisation, les ententes, le droit d'auteur et l'utilisation acceptable, et en a-t-on informé tout le personnel?**

Le conseil peut déléguer l'étude d'un certain nombre de ces points, ainsi que les questions à poser, au comité de vérification. Il va sans dire que la façon de procéder varie d'une organisation à l'autre. Le conseil peut s'acquitter de ses responsabilités quant aux points confiés au comité de vérification simplement en posant des questions à ce dernier et en discutant des réponses.

Un programme de suivi des réponses est indispensable. Si les réponses aux questions indiquent que des procédures seront mises en œuvre pour corriger les lacunes du système de contrôle, le conseil doit assurer un suivi lors de la réunion suivante pour déterminer si ces procédures ont bel et bien été mises en œuvre. Si le comité de vérification s'occupe de cet aspect en particulier, le rôle du conseil peut se limiter à établir que le comité a mis en place une procédure de suivi et qu'il n'a rien de nouveau à signaler. Si le comité de vérification n'a pas à s'occuper de cet aspect, les membres du conseil doivent faire une enquête auprès de la direction dans les meilleurs délais. Selon les résultats, d'autres mesures de suivi pourront être nécessaires ultérieurement.

Conclusion

Les technologies de l'information revêtent aujourd'hui une telle importance et sont devenues tellement complexes que, pour beaucoup d'organisations, une panne des systèmes informatiques peut signifier pratiquement un arrêt total des activités. Une mauvaise supervision des contrôles portant sur ces systèmes peut donc coûter très cher et entraîner dans certains cas des pertes commerciales importantes, la chute du cours des actions et, partant, une baisse de la capitalisation boursière. Le conseil a à cet égard une responsabilité très claire et très réelle.

De toute évidence, il incombe à tous les membres du conseil d'accorder une grande attention aux questions liées aux systèmes d'information. S'ils posent régulièrement les questions énoncées dans cette brochure, ils auront assumé une part importante de leurs responsabilités.

Stratégie

I Stratégie et planification

1. La direction a-t-elle un plan stratégique en matière de systèmes d'information qu'elle surveille et met à jour selon les besoins? Ce plan sert-il de base aux plans annuels, aux budgets annuels et à long terme, et à la priorisation des projets en technologies de l'information?

II Tendances technologiques

2. L'organisation a-t-elle mis en place des procédures appropriées pour se tenir au courant des tendances technologiques, pour les évaluer périodiquement et pour en tenir compte dans sa stratégie de positionnement?

III Performance

3. Les indicateurs et inducteurs de performance clés du service des TI ont-ils été établis? En fait-on régulièrement le suivi et les compare-t-on aux normes du secteur?
4. Les indicateurs pertinents ont-ils été établis et en fait-on le suivi pour assurer la gestion de la performance des tiers fournisseurs de services de l'organisation?

IV Personnel

5. Comment la direction a-t-elle déterminé l'expertise technologique nécessaire et quels moyens utilise-t-elle pour attirer les employés les plus talentueux?
6. La direction a-t-elle mis en place des procédures appropriées en matière de roulement, de formation et d'affectation des employés du service des technologies de l'information?

Contrôle interne

V Gouvernance

7. Le conseil a-t-il envisagé la création d'un sous-comité des TI ou a-t-il confié à l'un ou plusieurs de ses membres la responsabilité des investissements de l'organisation dans les TI et de leur utilisation?
8. La responsabilité de la gouvernance en matière de TI incombe-t-elle à une personne occupant un poste de direction suffisamment élevé? Comment la direction communique-t-elle les politiques de l'organisation en matière de TI aux employés?
9. Quelles sont les procédures mises en place pour assurer que les systèmes et la gestion de l'entreprise soient conformes aux exigences de la Loi Sarbanes-Oxley et/ou des règlements des ACVM visant à rétablir la confiance des investisseurs, le cas échéant?

Risques

VI Risques et contrôles

10. La direction planifie-t-elle des évaluations périodiques des risques liés à l'utilisation des technologies de l'information par l'organisation, et notamment aux systèmes et processus internes, à l'externalisation de services et au recours à des services de communications indépendants et à d'autres services? Le cas échéant, prend-elle les mesures appropriées ou nécessaires compte tenu des résultats de ces évaluations?
11. Comment la direction assure-t-elle l'intégrité des données et, par le fait même, leur pertinence, leur intégralité, leur exactitude, la rapidité de leur diffusion et leur utilisation judicieuse au sein de l'organisation?

12. Quelles dispositions ont été prises par l'organisation pour qu'aient lieu l'examen et la vérification périodiques de ses systèmes, afin d'assurer que les risques soient suffisamment atténués et que ses processus clés soient appuyés par des contrôles?

VII Protection des renseignements personnels

13. L'organisation a-t-elle nommé un responsable des politiques en matière de protection des renseignements personnels, des lois en la matière et du respect de celles-ci?
14. L'organisation a-t-elle identifié les diverses exigences contenues dans les textes législatifs et réglementaires quant à la protection des renseignements personnels et a-t-elle élaboré une politique et des procédures pour assurer leur respect?

VIII Affaires électroniques

15. Si l'organisation fait appel aux affaires électroniques pour acheter ou vendre des produits ou des services, a-t-elle fait faire un examen particulier des risques et des contrôles relatifs aux affaires électroniques?
16. Les activités d'affaires électroniques de l'organisation sont-elles suffisamment protégées contre une attaque externe ou interne par des personnes non autorisées ou d'autres personnes qui, en cas de réussite, se traduirait par une baisse de la satisfaction de ses clients ou porterait atteinte à son image publique?

IX Disponibilité

17. L'organisation a-t-elle adopté des politiques officielles relatives à la disponibilité? A-t-elle mis en œuvre des contrôles efficaces destinés à procurer une assurance raisonnable que les systèmes et les données sont disponibles en conformité avec ces politiques?
18. L'organisation comprend-elle l'incidence d'une interruption de service et a-t-elle mis en place des plans pour gérer les interruptions potentielles? A-t-elle adopté un plan de continuité de l'exploitation? Le cas échéant, ce plan fait-il l'objet de tests périodiques et l'améliore-t-on à la lumière des résultats?

X Aspects juridiques

19. La direction a-t-elle pris en considération et analysé les incidences juridiques relatives à l'utilisation des logiciels et du matériel, aux ententes de service et aux lois sur le droit d'auteur?
20. A-t-on formulé des politiques sur les permis d'utilisation, les ententes, le droit d'auteur et l'utilisation acceptable, et en a-t-on informé tout le personnel?

Au sujet des auteurs

Le Comité consultatif sur les technologies de l'information (CCTD) relève de la division Développement des connaissances de l'ICCA. Il joue un rôle de soutien et de conseil sur les questions de TI qui ont une incidence sur la profession de CA et sur le milieu des affaires.

Comité consultatif sur les technologies de l'information de l'ICCA

Président

Donald E. Sheehy, CA•CISA, Deloitte & Touche LLP, Toronto

Comité

Gary S. Baker, CA, Deloitte & Touche LLP, Toronto

David Chan, CA•CISA, Centre de protection de l'information, gouvernement de l'Ontario, Toronto

Allan W.K. Cheung, CA•TI, CISA, La Caisse canadienne de dépôt de valeurs limitée, Toronto

Henry Grunberg, CA•TI, Ernst & Young LLP, Toronto

Ray Henrickson, CA•TI/CISA, La Banque Scotia, Toronto

Carole Le Néal, CISA, Mouvement des caisses Desjardins, Montréal

James R. Murray, CA, CISA, Grant Thornton LLP, Halifax

Erlinda L. Olalia-Carin, CISA, KPMG LLP, Toronto

Robert G. Parker, FCA, CA•CISA, Deloitte & Touche LLP, Toronto

Robert J. Reimer, CA•CISA, PricewaterhouseCoopers LLP, Winnipeg

Douglas G. Timmins, CA, Bureau du vérificateur général du Canada, Ottawa

Gerald D. Trites, FCA, CA•CISA, St. Francis Xavier University, Antigonish (Nouvelle-Écosse)

(consultant contractuel affecté au Comité)

Bryan C. Walker, CA, L'Institut Canadien des Comptables Agréés, Toronto

Personnel de l'ICCA

William J.L. Swirsky, FCA, vice-président, Développement des connaissances

Andrée Lavigne, CA, directrice de projets, Monographies

ISBN 1-55385-123-4



9 781553 851233

20 Questions

que les administrateurs devraient poser sur
les technologies de l'information

Révision : avril 2004

277, rue Wellington Ouest
Toronto (Ontario)
Canada M5V 3H2
Téléphone : 416 977-0748
1 800 268-3793
Télécopieur : 416 204-3416
Internet : www.icca.ca

 L'Institut Canadien
des Comptables Agréés