CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Gouvernance des données et des TI

TENDANCE TECHNOLOGIQUE

« Selon moi, le facteur qui a le plus contribué au succès des TI, c'est la gouvernance des TI. »

—Peter Weill, président du Center for Information Systems Research, Massachusetts Institute of Technology

Description

La gouvernance des technologies de l'information (TI) s'entend de la gestion et du contrôle de l'environnement TI, notamment les données utiles à une organisation et à ses parties prenantes. Cette gouvernance, qui relève du conseil d'administration et de la haute direction, fait partie intégrante de la gouvernance d'entreprise. La gouvernance des TI exige un leadership, des structures organisationnelles, des politiques, des processus et des contrôles internes afin que les TI respectent la stratégie et les objectifs de l'organisation et de ses parties prenantes. En termes clairs, la gouvernance des TI englobe les efforts des employés et les processus qui soutiennent la prise de décisions relatives aux initiatives technologiques. Lorsqu'elle est mise en œuvre avec efficacité, cette gouvernance permet d'atteindre un équilibre entre la création de valeur et l'atténuation des risques pour l'entreprise.

Gouvernance des TI et gouvernance organisationnelle

L'Organisation de coopération et de développement économiques (OCDE) définit la gouvernance d'entreprise ou organisationnelle comme le système en vertu duquel les organisations sont dirigées et contrôlées. La structure de gouvernance organisationnelle précise la répartition des droits et des responsabilités entre les différents participants : le conseil d'administration, les sous-comités du conseil, la haute direction, la direction, les actionnaires et les autres parties prenantes. En outre, elle donne le ton en matière d'orientation et de gestion, établit et gère les objectifs, définit la culture et les valeurs, et détermine les processus, les procédures et les règles entourant la prise de décisions. La gouvernance organisationnelle fournit également une structure grâce à laquelle l'entreprise établit ses objectifs et détermine les moyens à prendre pour les réaliser. Elle définit également les principaux indicateurs de rendement et

d'atteinte des objectifs, ainsi qu'un processus de transmission des constatations et de mise en œuvre des améliorations et des changements.

Un élément essentiel pour assurer le succès de la gouvernance des TI est la communication régulière, avec les principales parties prenantes, sur l'avancement des plans stratégiques et tactiques en matière de TI. Cette communication mène à l'établissement d'un dialogue constructif qui favorise la transparence et permet d'identifier les secteurs où les risques sont susceptibles d'augmenter : retards opérationnels, dépassements de coûts, incapacité de concrétiser les avantages propres aux TI, démobilisation des parties prenantes, modifications du champ d'application, défis technologiques et manque de ressources. Qui plus est, en permettant à l'équipe TI d'avoir voix au chapitre, la communication avec le comité directeur, le comité d'audit, le comité de gestion des risques et le conseil d'administration devient claire et pragmatique, et l'organisation acquiert une compréhension rapide et suffisante de la valeur et des risques liés aux TI pour assurer la gouvernance efficace du conseil et de la haute direction.

Les plans stratégiques et tactiques relatifs aux TI sont souvent considérés comme un exercice ponctuel ou élaborés sans tenir compte des plans stratégiques de l'entreprise; ils font rarement l'objet d'une surveillance et de communications régulières. Par conséquent, ces plans, mal coordonnés, ne répondent pas aux besoins des initiatives actuelles, nouvelles ou éventuelles

EXEMPLE DE SYNERGIE ENTRE L'ENTREPRISE ET LES TI RENFORÇANT LA CRÉATION DE VALEUR

Un détaillant en ligne définit comme besoin stratégique d'accroître ses ventes et d'augmenter sa rentabilité, tâche qui lui semble difficile en raison de la concurrence. La direction a recours aux données de marché produites par l'entreprise elle-même et à des données achetées auprès de chercheurs externes, afin de relever des récurrences et des comportements permettant de cerner les occasions de mener à bien la stratégie organisationnelle. Un fournisseur de services infonuagiques est engagé pour collaborer avec l'entreprise et son équipe TI à la personnalisation du contenu des produits, à l'offre de rabais adaptés à la clientèle et à la formulation de suggestions concernant d'autres produits. En utilisant des outils sophistiqués de veille stratégique et en tirant parti des données et des systèmes TI internes et externes, ce détaillant en ligne parvient à proposer à ses clients des produits qui répondent à leurs besoins, tout en augmentant leur satisfaction et en réduisant le nombre de produits retournés. Ainsi, l'entreprise atteint ses objectifs stratégiques d'expansion de ses activités en dépassant ses cibles de ventes et de profit, en diminuant le coût des retours et en fidélisant sa clientèle. De plus, l'équipe TI collabore étroitement avec les équipes internes du marketing, du service juridique, des finances et de l'exploitation, ainsi qu'avec le fournisseur de services infonuagiques, pour veiller au respect de l'ensemble des lois et des règlements.

de l'entreprise. En mettant l'accent sur les enjeux opérationnels liés aux TI plutôt que sur les questions stratégiques plus vastes, on risque de manquer des occasions de créer de la valeur pour l'entreprise.

Mise en œuvre correctement et efficacement, la gouvernance des TI permet aux TI d'orienter les initiatives organisationnelles et les stratégies d'entreprise. Elle crée un environnement où l'organisation peut tirer pleinement parti de ses ressources TI pour créer de la valeur et la préserver, obtenir un avantage concurrentiel et atteindre ses objectifs stratégiques. De plus, elle augmente la probabilité que l'équipe TI fournisse ses services en respectant le cadre et le budget prévus. Malheureusement, de nombreuses entreprises peinent à comprendre et à encadrer la fonction TI, ainsi que les processus et les activités qui lui sont propres. Cette incapacité à saisir pleinement les avantages qu'offrent les processus, les technologies, les initiatives et le personnel des TI peut mener à une perte de valeur et à une augmentation des risques pour l'entreprise.

Importance

Gouvernance des TI

Depuis que les technologies, les données et l'information sont devenues des moteurs de l'innovation et de la création de valeur pour les entreprises, le rôle des TI a évolué. De ce fait, une solide gouvernance est requise pour utiliser efficacement les ressources TI dans le but d'appliquer la stratégie d'entreprise et d'atténuer les nouveaux risques. En établissant une gouvernance efficace des TI, l'entreprise est en mesure de développer une culture et un modèle opérationnel adaptés, et en mettant bien en place cette gouvernance, elle peut tirer de la valeur des opérations et des investissements relatifs aux TI. Ainsi, la vision, la stratégie, les programmes, les initiatives et les plans de l'entreprise s'harmonisent avec les plans et les tactiques nécessaires à leur réalisation. Comme les employés, les processus et les technologies vont dans la même direction – celle du progrès de l'entreprise –, cette dernière peut atteindre et même dépasser ses objectifs.

QUEL EST LE RÔLE DES CPA DANS LA GOUVERNANCE DES TI?

Lorsqu'ils siègent au conseil ou à des comités, les CPA doivent comprendre la gouvernance des TI même s'ils ne feront que rarement partie de la structure ou du processus de cette gouvernance. Habituellement, le conseil et les comités doivent approuver les niveaux globaux de tolérance au risque, dont les risques liés aux TI comme la protection des renseignements personnels, la cybersécurité et la continuité des activités. Ils doivent aussi approuver la répartition des ressources, dont les ressources TI, ainsi que les objectifs de rendement et les stratégies globales, dont les objectifs propres aux TI, pour l'organisation. Dans cette optique, les CPA doivent avoir une compréhension globale des tendances et des enjeux liés aux TI.

Les CPA jouent aussi un rôle essentiel en ce qui a trait à la gouvernance des TI pour les programmes et les projets. En effet, certains programmes peuvent être des initiatives fondées sur les TI ayant une incidence sur les activités de l'organisation, comme dans le cas de la cybersécurité. Par exemple, le fait de cesser toute activité lorsqu'une cybermenace est imminente peut avoir des répercussions sur la sécurité du personnel ou des clients. La prise d'une telle décision ne relève pas que de l'équipe TI. Les CPA doivent donc veiller à ce qu'il y ait une représentation appropriée de la haute direction et à ce que le processus relatif à ces types de programmes soit testé régulièrement afin que l'organisation soit fin prête en cas d'urgence.

Pour ce qui est des projets, les CPA doivent faire partie de l'équipe de gouvernance du projet avec les responsables de l'équipe TI et de l'entreprise ayant demandé le projet. Ils doivent prendre part à la réalisation d'analyses de rentabilité et à l'établissement de budgets, s'assurer de la présence de représentants de l'équipe TI et de l'entreprise au sein de l'équipe du projet, mais ne pas oublier que le processus décisionnel dans son ensemble repose entre les mains de l'entreprise.

Sans CPA pour assurer une bonne gouvernance, les projets et les programmes TI peuvent n'être axés que sur les TI et ne pas avoir le soutien de l'entreprise. Le projet risque alors de ne plus s'arrimer à la vision et à la stratégie de l'entreprise et, ainsi, d'être voué à l'échec.

Gouvernance des données

Vu l'émergence de techniques d'analyse sophistiquées et d'ordinateurs possédant une énorme puissance de calcul, il est désormais possible de fonder des décisions sur les données. Ainsi, les données ont une très grande valeur pour les entreprises. Et en raison de l'importance croissante des données et de leur utilisation dans un environnement TI, on comprendra que les TI ont un rôle essentiel à jouer dans ce nouveau secteur. Ainsi, lorsqu'on parle de gouvernance des TI, il faut également tenir compte de la gouvernance des données. Bien que de nombreuses personnes affirment que les données « appartiennent » à une entreprise, la notion de propriété des données doit être adaptée à la culture et à la structure de l'ensemble de l'organisation. Certains avanceront que, en raison de l'expertise de l'équipe TI en matière de protection des ressources TI de l'organisation, la propriété des

données devrait lui revenir. Toutefois, quel que soit le propriétaire des données, il convient de traiter celles-ci comme l'une des plus précieuses ressources de l'organisation. Des contrôles internes appropriés doivent donc être mis en place pour protéger les données contre les cyberattaques, les vols et les détournements, ainsi que les infractions aux lois et règlements en matière de protection des renseignements personnels, notamment. L'équipe TI a un rôle important à jouer en tant que partenaire stratégique dans l'amélioration de l'intégrité, de la sécurité et de l'exhaustivité des données afin d'étayer la prise de décision, ainsi que dans la gestion des données comme ressource stratégique clé.

Avantages et considérations pour les entreprises

Voici les avantages, pour une entreprise, de mettre en place un programme de gouvernance des TI et des données :

- Meilleurs arrimage et exécution des stratégies de l'entreprise et de celles des TI;
- Création de valeur par l'atteinte des objectifs de l'entreprise et des parties prenantes;
- Soutien technique et relatif aux systèmes afin d'assurer le respect des lois et des règlements;
- Renforcement de la sécurité des données et des ressources TI;
- Amélioration de la collaboration, du partage de données et, par conséquent, du processus décisionnel de l'entreprise;
- Réduction des coûts grâce à une gestion des risques plus efficace découlant des initiatives de TI;
- Reddition de comptes accrue en ce qui concerne la gestion du portefeuille et du programme TI.

Pour tirer pleinement parti de ces avantages, les organisations doivent mettre en place une stratégie visant à éviter certains des écueils courants associés aux programmes inefficaces de gouvernance des TI et des données. Le tableau ci-dessous résume ces secteurs de risque et propose des stratégies d'atténuation appropriées.

Secteurs de risque	Stratégies d'atténuation des risques
Il n'y a pas de stratégie globale et complète de gouvernance des données et des TI.	• Élaborer et adopter une stratégie de gouvernance des données et des TI fondée sur une norme reconnue ou un cadre et qui s'applique à l'ensemble de l'entreprise. • En ce qui concerne les cadres de gouvernance des TI, envisager l'utilisation de la norme ISO/IEC 38500:2015 de l'Organisation internationale de normalisation, ou du référentiel COBIT 2019, qui intègre plusieurs cadres, dont la norme ISO/IEC 38500:2015, et des cadres de gestion des données. • Envisager l'utilisation des cadres de gouvernance des données du Data Governance Institute (DGI). De nombreux fournisseurs de logiciels très connus (comme Microsoft, IBM, SAS et Oracle) ont publié des dossiers d'information sur la gouvernance des données.
L'entreprise ne parvient pas à respecter les nouvelles lois et les nouveaux règlements qui exigent la mise en place de processus et de systèmes sophistiqués pour assurer la surveillance de la conformité.	• Établir les besoins en matière de surveillance de la conformité aux lois et aux règlements (comme la *Loi sur la protection des renseignements personnels et les documents électroniques* – LPRPDE; *la Loi sur la protection des renseignements personnels,* la *Health Insurance Portability and Accountability Act* – (HIPAA); le Règlement général sur la protection des données (RGPD) de l'Union européenne (UE) et la *California Consumer Privacy Act* de 2020). • Envisager de mettre en place et de tester des procédures, nouvelles ou révisées, pour assurer le respect des lois et des règlements applicables (comme les exigences de suppression des données structurées et non structurées).
L'entreprise n'a pas les programmes et les plans nécessaires pour soutenir les initiatives de gouvernance des données et des TI qu'elle a prévues.	• Élaborer des plans TI tactiques avec un échéancier et des jalons clés afin d'assurer le respect du plan TI stratégique par l'entreprise, notamment son adoption par l'équipe TI et les utilisateurs.
La vision des TI ainsi que sa valeur et son utilité pour les parties prenantes et l'entreprise ne sont pas bien comprises.	• Créer un plan de communication relatif aux TI, et peut-être un comité directeur sur les TI composé de parties prenantes importantes et d'experts en TI rompus aux communications à l'échelle de l'entreprise.

Secteurs de risque	Stratégies d'atténuation des risques
La gouvernance des données et des TI n'a pas le champ d'application, l'application ou le soutien qui conviennent à l'échelle de l'organisation.	• Établir un conseil interfonctionnel sur la gouvernance des données comprenant les rôles clés suivants : intendant d'actif informationnel, architecte des données, chef de la qualité des données, chef de la technologie, chef de l'application, dirigeants d'entreprise et experts du domaine. • Lancer et mener une campagne de sensibilisation à la gouvernance des TI, enrichie de formation aux principales parties prenantes.
Les initiatives TI ne s'harmonisent pas avec les objectifs des parties prenantes ni avec les initiatives, les objectifs et les plans stratégiques de l'entreprise.	• Mettre en œuvre une stratégie TI qui comprend des plans annuels et tactiques arrimés aux objectifs des principales parties prenantes et aux initiatives, aux objectifs et aux plans stratégiques de l'entreprise.
Les pratiques en matière de surveillance de la performance liées à la gouvernance n'ont pas été mises en œuvre.	• Choisir les principaux objectifs et indicateurs de performance, et établir un processus de surveillance pour rendre compte aux parties prenantes des niveaux de développement et de performance et évaluer ces niveaux.
Les activités de surveillance et la prise de mesures correctives ne sont pas consignées et, par conséquent, on ne rend aucunement compte des activités de gouvernance des données et des TI.	• Mettre en place un processus pour consigner les activités faisant l'objet d'une surveillance et en informer les personnes appropriées à l'aide de tableaux de bord ou de rapports réguliers, aux fins de suivi et de résolution de problèmes. • Surveiller l'efficacité du conseil sur la gouvernance des données en examinant les améliorations et l'exactitude des rapports, la réduction du nombre de sources de données superflues et en double, et la centralisation et le stockage des données dans un entrepôt ou un lac de données.
L'équipe TI n'a pas adopté une méthode de gestion par portefeuille pour s'occuper des projets, des ressources et des initiatives TI.	• Choisir et mettre en œuvre une méthode de gestion du portefeuille TI dans le cadre de l'initiative de gouvernance des TI.
L'équipe TI n'a pas l'occasion ou ne tire pas parti des occasions de prendre contact avec le conseil d'administration, les sous-comités du conseil et la haute direction.	• Veiller à ce que l'équipe TI planifie la préparation de rapports réguliers pour le conseil, les sous-comités du conseil et la haute direction afin que les risques, les aspects complexes et les défis soient bien compris et surveillés. • Faire savoir aux parties prenantes qu'elles recevront de l'équipe TI des rapports réguliers et en temps utile.

Secteurs de risque	Stratégies d'atténuation des risques
Les plans TI ne traitent pas de création de valeur ni de gestion des risques.	• Intégrer la gestion de la valeur et des risques (ISO 31000 ou COBIT 2019) dans le champ d'application du plan stratégique TI, notamment les initiatives de gestion de la valeur et des risques. • Évaluer les risques émergents et les nouvelles technologies qui contribueront à réduire ces risques.
L'équipe TI n'a pas arrimé les efforts du personnel, les processus et les technologies aux risques de non-respect des lois et des règlements.	• Veiller à ce que les TI soient arrimées aux risques propres à l'entreprise en matière de non-respect des lois et des règlements. Préparer le personnel, les processus et les technologies TI de manière à réduire les risques résiduels de non-respect des lois et des règlements à un niveau acceptable.
L'équipe TI n'a pas géré et évalué correctement les risques liés au recours à des fournisseurs de services externes.	• Surveiller les risques découlant de la sous-traitance des services TI, notamment les services d'infonuagique offerts selon un modèle de logiciel-service (*SaaS*) et d'infrastructure-service (*IaaS*), en obtenant des rapports System and Organization Controls (SOC 1 et SOC 2) du fournisseur de services. • Évaluer si les rapports SOC et les contrôles internes de l'entreprise sont suffisants pour réduire à un niveau acceptable les risques pour l'entreprise.
L'équipe TI n'a pas l'occasion de surveiller, de gérer et de réduire les risques liés à la cybersécurité pour les parties prenantes à un niveau acceptable.	• Choisir et mettre en place un cadre de cybersécurité. Surveiller l'efficacité opérationnelle des contrôles internes en fonction de ce cadre. • Envisager l'utilisation du Cadre de cybersécurité du National Institute of Standards and Technology (NIST) et du programme Critical Security Controls du Center for Internet Security (CIS). • Envisager de souscrire une assurance cybersécurité afin de couvrir le risque résiduel à des niveaux supérieurs à ceux jugés acceptables par les parties prenantes.

Secteurs de risque	Stratégies d'atténuation des risques
L'équipe TI n'a pas la capacité de surveiller et de gérer les risques associés aux fournisseurs de services infonuagiques.	• Obtenir du fournisseur de services infonuagiques une autoévaluation qui utilise le Cloud Controls Matrix de la Cloud Security Alliance. • Obtenir du fournisseur de services infonuagiques un rapport d'audit SOC 1 (type 2) ou SOC 2 (type 2) pour déterminer si des contrôles suffisants ont été mis sur pied par le fournisseur afin de réduire les risques à un niveau acceptable pour les services offerts à votre organisation. • Examiner les contrôles de l'entité utilisatrice indiqués dans le rapport ci-dessus, et déterminer si les contrôles de l'entité utilisatrice de votre organisation combinés à ceux indiqués dans le rapport d'audit SOC 1 ou SOC 2 sont suffisants pour réduire à un niveau acceptable les risques auxquels s'expose votre organisation. • Définir des mesures clés prédictives (si possible) pour surveiller la performance de votre fournisseur de services infonuagiques. Intégrer ces mesures du rendement dans l'entente de niveau de service (ENS), et veiller au respect des mesures définies.

Conclusion

L'importance des technologies de l'information dans la stratégie et les objectifs d'une organisation s'est considérablement accrue. Les organisations soucieuses de saisir pleinement les avantages qu'offrent leurs ressources TI doivent mobiliser le personnel, les processus et les technologies en vue de la réalisation des mêmes objectifs. Et pour ce faire, il leur est essentiel de se doter d'un programme efficace de gouvernance des TI et des données.

La présente publication s'inscrit dans la **série Tendance technologique**, qui porte sur les grandes tendances du domaine touchant le milieu comptable. Les documents de cette série sont disponibles sur notre site Web.