VÉRIFICATEUR GÉNÉRAL DU QUÉBEC

Rapport du Vérificateur général du Québec
à l'Assemblée nationale pour l'année 2012-2013

Vérification de l'information financière
et autres travaux connexes

Hiver 2013

CHAPITRE

9

Contrôles généraux des technologies de l'information

Faits saillants

Objectifs des travaux

Les contrôles généraux des technologies de l'information (CGTI) sont cruciaux dans le processus de préparation des états financiers. Ce chapitre vise donc, d'une part, à mieux saisir l'importance pour les entités auditées de mettre en application les recommandations qui s'y rapportent et, d'autre part, à comprendre la démarche d'audit des CGTI qui conduit à la communication des déficiences liées à la gestion des technologies de l'information dans un rapport aux responsables de la gouvernance et à la direction.

Dans un premier temps, nous situons les CGTI dans le processus de préparation des états financiers. Puis, nous présentons de façon sommaire l'approche d'audit des CGTI appliquée par le Vérificateur général du Québec (VGQ) dans le cadre de l'attestation annuelle des états financiers ainsi que les normes et standards attendus chez les entités auditées. À partir d'un portrait des recommandations touchant les différents sujets relatifs aux CGTI formulées au cours des dernières années, nous terminons le chapitre en présentant l'importance pour les entités de les mettre en application.

Le rapport entier est disponible sur le site : http://www.vgq.qc.ca

Résultats des travaux

Nous présentons ci-dessous les principaux éléments ressortant de nos travaux portant sur l'audit des contrôles généraux des technologies de l'information dans le cadre de l'attestation des états financiers.

Les CGTI sont un des fondements du contrôle interne d'une entité, du fait qu'ils affectent tout le processus de production des états financiers des entités auditées. Ce lien étroit entre les deux fait en sorte que la fiabilité du fonctionnement des CGTI garantit le degré de confiance acceptable que nous sommes en mesure d'accorder à l'ensemble des contrôles liés aux applications informatiques et à l'infrastructure technologique qui les supporte, et ce, tout au long d'un exercice financier.

Selon l'approche d'audit des CGTI adoptée au VGQ, nous portons une attention particulière aux contrôles relatifs à la gestion du développement et de la maintenance des systèmes, à celle des droits et des profils d'accès, ainsi qu'à celle des paramètres de sécurité, du fait de leur impact majeur sur l'intégrité des données financières. Toute déficience significative de l'un des contrôles clés liés à ces CGTI représente un risque important à cet égard, empêchant souvent l'utilisation d'une stratégie d'audit des états financiers basée sur les contrôles informatiques, ce qui entraine une recommandation dans un rapport aux responsables de la gouvernance et à la direction.

Malgré le risque élevé sur l'intégrité des données, les entités tardent à appliquer nos recommandations liées à la gestion des technologies de l'information (TI) bien qu'elles y adhèrent. Le taux d'application des recommandations en ce qui a trait à la gestion des TI est demeuré faible (53 à 55 %) au cours des trois dernières années.

Une large part de nos recommandations liées à la gestion des TI concernent le Centre de services partagés du Québec (CSPQ). La diversité des systèmes et des infrastructures technologiques ainsi que l'étendue de sa clientèle peuvent expliquer cette situation. Conscient de cette problématique, le Centre a déjà entrepris des actions concrètes pour remédier d'ici le 31 décembre 2013 à la majorité des déficiences mentionnées dans nos rapports. Nous y porterons une attention particulière au cours des années à venir.

Table des matières

Équipe

Martin Lessard
Directeur

Claude Dion
Patrice Watier

1 Mise en contexte

1 Dans le *Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2012-2013* et portant sur la *Vérification de l'information financière et autres travaux connexes*, le chapitre 8 dresse pour une troisième année consécutive un portrait des rapports aux responsables de la gouvernance et à la direction produits du 1er octobre 2011 au 30 septembre 2012.

2 Le taux d'application des recommandations en ce qui a trait à la gestion des technologies de l'information (TI) est demeuré faible (53 à 55 %) au cours des trois dernières années.

3 Cette situation nous préoccupe. C'est pourquoi nous présentons dans le présent chapitre une analyse plus approfondie de nos travaux concernant les contrôles généraux des technologies de l'information (CGTI) dans le contexte de nos mandats d'audit financier.

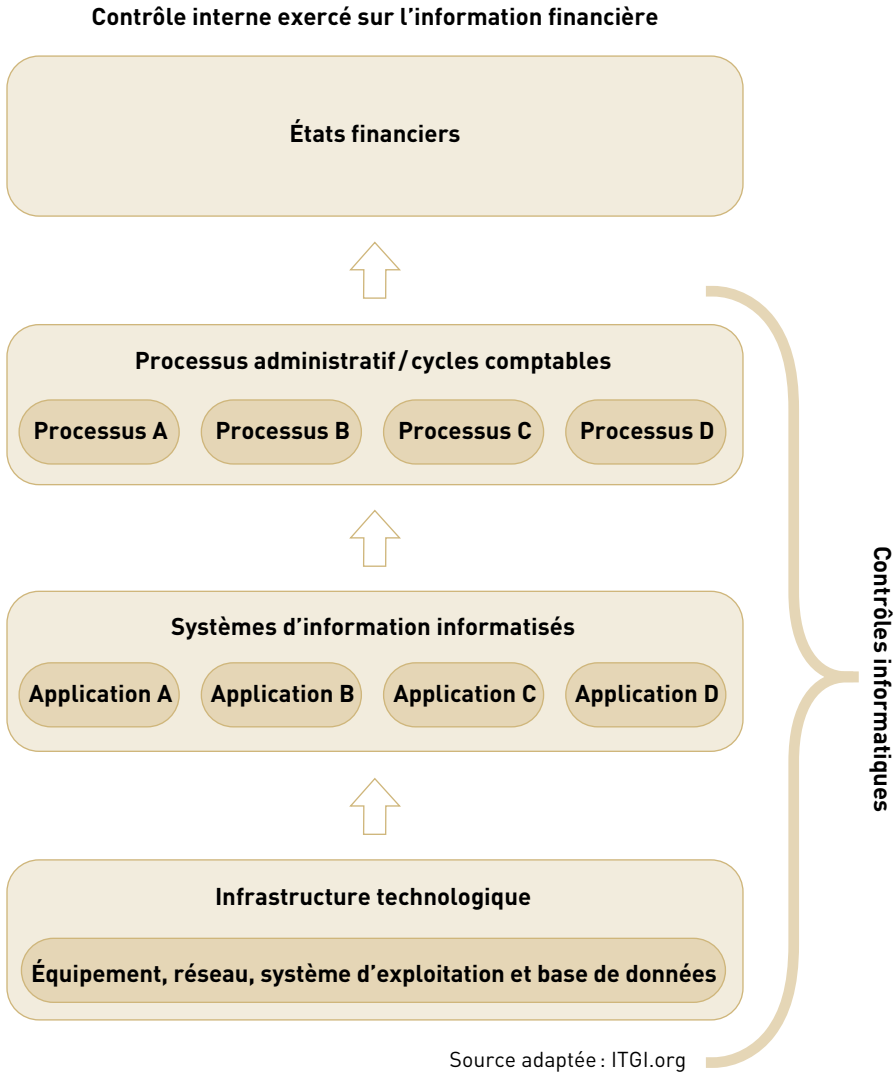
2 Résultats des travaux

2.1 Importance des CGTI dans le processus de préparation des états financiers

4 Les CGTI sont un des fondements du contrôle interne de l'entité et ils affectent tout le processus de production des états financiers d'une entité. Ce lien étroit entre les deux fait en sorte que la fiabilité du fonctionnement des CGTI garantit le degré de confiance acceptable que nous sommes en mesure d'accorder à l'ensemble des contrôles liés aux applications informatiques et à l'infrastructure technologique qui les supporte, et ce, tout au long d'un exercice financier.

5 Dans le processus de préparation des états financiers des entités auditées par le Vérificateur général du Québec (VGQ), la quasi-totalité des transactions de nature financière sont traitées à l'aide d'applications informatisées. Ainsi, les TI sont souvent à la base de la préparation des états financiers, comme le démontre le diagramme de la figure 1.

Figure 1 **Diagramme des principaux éléments de base d'un système d'information nécessaires à la production des états financiers**



Source adaptée : ITGI.org

6 Pour répondre aux risques découlant du recours aux TI et assurer un fonctionnement efficace et continu des applications informatiques et de l'infrastructure technologique qui les supporte, l'entité doit mettre en place un ensemble de contrôles informatiques, incluant les CGTI, qui couvrent tous les systèmes d'information de l'organisation. Dans le cadre de l'audit des états financiers, nous nous attardons uniquement aux systèmes qui ont un impact sur la production des états financiers, ce qui peut exclure parfois certains systèmes d'information liés à la mission des entités auditées, tels qu'un système de gestion de l'entretien des infrastructures routières ou encore de gestion des effectifs scolaires. Les CGTI comprennent un ensemble de politiques et de procédures encadrant la sécurité de l'information et les processus relatifs, notamment, à la gestion du développement et de la maintenance des systèmes ainsi qu'à la gestion des accès.

CGTI et sécurité de l'information

7 Lors de l'audit des CGTI, nous portons une attention particulière aux contrôles assurant l'intégrité des données financières.

8 Des CGTI fiables et efficaces, assurant le maintien d'un niveau adéquat de sécurité de l'information, représentent un des principaux enjeux du contrôle interne d'une organisation. Cette sécurité de l'information s'évalue selon trois objectifs : la disponibilité, l'intégrité et la confidentialité.

- Disponibilité : garantir que les systèmes sont accessibles au moment voulu par les personnes autorisées. Les systèmes doivent fonctionner sans faille durant les périodes d'utilisation prévues et garantir, selon les besoins, l'accès en temps opportun aux services et aux ressources installées.
- Intégrité : prévenir que les données, lors de leur traitement, de leur conservation ou de leur transmission, ne seront pas altérées ou détruites de façon fortuite ou volontaire, afin d'en assurer l'exhaustivité, l'exactitude et l'authenticité.
- Confidentialité : assurer que seules les personnes autorisées peuvent accéder en mode lecture à des fins de consultation aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

9 Dans le cadre d'un audit des états financiers, l'objectif lié à l'intégrité des données est le plus important, car il concerne la fiabilité des données financières. Certains éléments ayant trait à la disponibilité des systèmes sont examinés en vue d'assurer la continuité des opérations des entités auditées. En ce qui concerne la confidentialité de l'information, il faut comprendre que le fait qu'une personne non autorisée puisse accéder en mode lecture seulement à de l'information jugée confidentielle pour l'entité ne représente pas un risque d'altérer les données financières. Cependant, cet objectif demeure important pour les entités, notamment dans un contexte de protection des renseignements personnels.

2.2 Audit des CGTI selon l'approche adoptée par le VGQ

10 L'approche d'audit des CGTI adoptée par le VGQ est conforme aux Normes d'audit généralement reconnues du Canada qui incluent les Normes canadiennes d'audit. De plus, elle s'appuie sur plusieurs référentiels supportés par des organismes reconnus internationalement, principalement le CobiT de l'ISACA[1]. Enfin, nous visons à améliorer nos pratiques de façon continue, soit par une vigie des méthodologies établies par les autres auditeurs législatifs du Canada,

1. « Control Objectives for information and related Technology » publié par l'« Information Systems Audit and Control Association ».

soit à travers nos collaborations avec les grands cabinets d'experts-comptables avec lesquels nous travaillons en co-audit ou dans le cadre des mandats confiés en impartition.

11 Notre approche d'audit des CGTI est basée sur une méthodologie qui regroupe un ensemble de procédés d'audit appliqués à l'environnement informatique. Elle couvre cinq sujets relatifs à la gestion des TI, soit :

- la politique et les procédures de sécurité ;
- la gestion du développement et de la maintenance des systèmes ;
- la gestion des droits et des profils d'accès ;
- la gestion des paramètres de sécurité ;
- la gestion des opérations.

12 Les contrôles liés à la gestion du développement et de la maintenance des systèmes, à la gestion des droits et des profils d'accès ainsi qu'à la gestion des paramètres de sécurité ont un impact majeur sur l'intégrité des données financières. Toute déficience significative de l'un des contrôles clés relatifs à ces CGTI représente donc un risque important à cet égard, empêchant souvent l'utilisation d'une stratégie d'audit des états financiers basée sur les contrôles informatiques, ce qui entraine une recommandation dans un rapport aux responsables de la gouvernance et à la direction.

Politique et procédures de sécurité

13 La mise en place par les entités auditées d'une politique et de procédures de sécurité est un des éléments importants de notre méthodologie. Elles établissent, en matière de sécurité, les principes de base qui sous-tendent les autres sujets relatifs à la gestion des TI.

14 La direction doit témoigner d'une préoccupation constante quant à l'ensemble de son contrôle interne, notamment en ce qui concerne les contrôles liés aux TI. Pour nous en assurer, nous procédons à l'identification des facteurs de risque pouvant entrainer des anomalies significatives ayant un impact sur les états financiers de l'entité auditée. L'application d'une politique de sécurité est l'un des facteurs importants que nous considérons, car elle énonce les principes directeurs et établit les rôles et les responsabilités des principaux intervenants en matière de sécurité de l'information. Nous nous assurons que l'entité s'est dotée d'une telle politique, qu'elle est soutenue par des procédures de sécurité et qu'elle est diffusée auprès de tout le personnel de l'organisation. Le maintien d'activités de surveillance et de reddition de comptes, comme la mise en place d'un comité de sécurité, est également un élément à prendre en compte.

15 Une déficience en ce qui a trait, entre autres, à l'absence d'une politique de sécurité de l'information, n'affecte pas directement l'intégrité des données financières ni la stratégie d'audit adoptée. Toutefois, elle est communiquée dans un rapport aux responsables de la gouvernance et à la direction, du fait de son impact sur les autres sujets liés aux CGTI.

Gestion du développement et de la maintenance des systèmes

16 La gestion du développement et de la maintenance des systèmes comprend les contrôles liés au développement et à l'acquisition de nouveaux systèmes, de même que la maintenance des systèmes existants, ainsi que des bases de données et de l'infrastructure technologique qui les supportent.

17 Toute déficience significative en ce qui a trait à la gestion du développement et de la maintenance des systèmes augmente le risque que des modifications non autorisées soient apportées aux programmes ou aux données financières, ou que des modifications nécessaires ne soient pas réalisées ou ne soient pas effectuées adéquatement.

18 Dans le cadre de l'audit des états financiers, les modifications apportées aux systèmes d'information de nature financière représentent un risque important quant à l'intégrité des données. Notre audit sur l'efficacité de ces CGTI vise donc à nous assurer que l'entité a mis en place des processus adéquats, comprenant au minimum les contrôles suivants, qui respectent les saines pratiques de gestion dans ce domaine :

- Les modifications apportées aux programmes informatiques par les analystes-programmeurs sont effectuées dans un environnement de développement distinct des environnements de test et de production.
- Les essais servant à s'assurer que les programmes informatiques modifiés donnent les résultats attendus sont généralement réalisés par une équipe représentant les utilisateurs. Ils sont également effectués dans un environnement de test distinct de celui de production, et ce, pour être certain de ne pas altérer les données financières.
- Une autorisation de migrer en production les programmes informatiques est obtenue du responsable des utilisateurs en temps opportun.
- La migration des programmes informatiques de l'environnement de test vers l'environnement de production est effectuée par du personnel différent de celui qui fait la programmation et de celui qui réalise les essais, respectant ainsi le principe de séparation des tâches incompatibles.
- La documentation des systèmes est mise à jour dans le but de faciliter leur entretien dans le futur.

19 Les mêmes contrôles doivent être mis en place lors de l'implantation d'un nouveau système informatique, ce qui implique généralement une conversion de données, car cette situation représente également un risque important quant à l'intégrité des données financières.

20 Enfin, toutes modifications aux données financières effectuées directement dans une base de données en production sans passer par une application informatisée représentent un risque majeur en ce qui concerne l'intégrité des données ; l'entité doit s'assurer qu'elles sont :

- autorisées et réalisées par le personnel approprié ;
- journalisées afin de permettre des vérifications a posteriori.

Gestion des accès

21 La gestion des accès regroupe les deux prochains sujets, soit la gestion des droits et des profils d'accès ainsi que la gestion des paramètres de sécurité. La gestion des accès comprend, d'une part, les contrôles d'accès physiques à l'infrastructure technologique qui supporte les systèmes informatiques et, d'autre part, les contrôles d'accès logiques permettant aux utilisateurs d'accéder aux applications informatisées ; ce dernier type étant considéré comme le plus crucial pour assurer l'intégrité des données.

22 Des mécanismes de sécurité et des contrôles d'accès physiques aux salles informatiques doivent être mis en place par les entités, pour assurer une protection adéquate de l'infrastructure technologique qui supporte les systèmes informatiques. Elles doivent veiller au minimum à ce que :

- les accès physiques soient limités au personnel autorisé, habituellement un groupe restreint du personnel du service informatique (portes verrouillées, caméras de surveillance, registre d'accès à des fins de suivi, etc.) ;
- des mécanismes de sécurité adéquats soient mis en place (climatisation, détecteurs de fumée, etc.) afin d'assurer la disponibilité des systèmes et des données.

23 Quant aux contrôles d'accès logiques, ils reposent sur deux concepts fondamentaux, soit l'identification des individus voulant accéder au système informatique et l'authentification de ces personnes par le système.

- L'identification vise à ce que seules les personnes autorisées aient accès aux systèmes informatiques, et que cet accès soit restreint aux informations qui leur sont nécessaires. Ce principe exige que chaque personne ait un code d'identité unique et que des droits et des profils d'accès y soient associés afin de déterminer les données auxquelles le détenteur peut accéder en fonction du poste qu'il occupe.
- L'authentification vise à valider l'identité d'une personne en s'assurant que cette personne est bien celle qu'elle prétend être selon le code d'identité qu'elle fournit. Diverses méthodes peuvent être appliquées, notamment l'utilisation de mots de passe, de carte à puce ou de mesures biométriques.

24 La gestion des droits et des profils d'accès, qui est liée à l'identification d'un individu, ainsi que la gestion des paramètres de sécurité des mots de passe, laquelle concerne l'authentification de celui-ci, s'avèrent donc être des processus cruciaux pour une organisation.

25 Toute déficience significative en ce qui concerne la gestion des accès, tant celle des droits et des profils d'accès que celle des paramètres de sécurité, augmente le risque d'accès non autorisé aux données, ce qui peut conduire à leur destruction ou à des modifications inappropriées, y compris l'enregistrement d'opérations non autorisées ou inexistantes.

26 Notre audit sur l'efficacité de ces contrôles vise donc à nous assurer que l'entité a mis en place un processus adéquat de gestion des accès logiques aux applications informatisées, comprenant les contrôles qui respectent les saines pratiques de gestion dans ce domaine.

Gestion des droits et des profils d'accès

27 Pour la gestion des droits et profils d'accès, nous devons retrouver au minimum les contrôles suivants :

- Une autorisation formelle est obtenue, généralement du gestionnaire de la personne, avant l'octroi des codes d'identité et des droits d'accès y afférents lors de l'arrivée d'un nouvel employé.
- Une révocation des anciens droits d'accès est faite en temps opportun lors d'un mouvement de personnel à l'intérieur de l'organisation. Les nouveaux droits d'accès doivent également être autorisés.
- Une révocation des codes d'identité est faite en temps opportun lors du départ d'un employé.
- Aucun code d'identification ne doit représenter un compte utilisé par un groupe de personnes, et ce, afin de rendre chaque utilisateur responsable des interventions qu'il effectue avec son code.
- Une révision périodique des droits d'accès est faite par les responsables des différents services. Dans ce cas, il importe de s'assurer que le principe de séparation des fonctions incompatibles est respecté entre la personne qui autorise et révise les droits d'accès et celle qui les octroie.

28 Certaines personnes se voient attribuer des codes possédant des accès privilégiés, ce qui leur procure des pouvoirs plus étendus (administrateur de réseau ou de bases de données, etc.) que les utilisateurs réguliers. Outre les contrôles énumérés précédemment, les entités doivent veiller à ce que :

- le nombre de personnes bénéficiant de ces codes soit restreint au minimum, en fonction de leurs tâches régulières ;
- l'utilisation de ces codes fasse l'objet d'un suivi périodique et documenté par une personne indépendante.

29 En ce qui concerne les contrôles des accès externes, ils sont audités seulement s'il subsiste un risque significatif d'accéder, en ayant recours à l'Internet, aux applications financières importantes ou aux applications de commerce électronique importantes telles que la vente de billets de loterie ou le remboursement de frais médicaux. Dans ce cas, nous devons nous assurer que des mécanismes de contrôle adéquats sont mis en place afin de sécuriser les accès externes aux systèmes contenant les données financières importantes.

Gestion des paramètres de sécurité

30 Pour ce qui est de la gestion des paramètres de sécurité, il est à noter que l'utilisation de mots de passe est le mécanisme qui est le plus couramment utilisé par nos entités auditées afin d'authentifier un individu qui veut accéder à leurs systèmes informatiques. Leur configuration doit respecter des standards qui, au fil des années, ont été rehaussés du fait que les outils pour les capturer se sont également améliorés. Actuellement, les principales normes adoptées par le VGQ sont les suivantes :

- La longueur des mots de passe doit être de huit caractères au minimum.
- Leur composition doit comprendre une combinaison de lettres, minuscules et majuscules, de chiffres ou de caractères spéciaux, tels /*@#$.
- Le nombre de tentatives d'accès infructueux avant la désactivation du code d'accès doit être limité à trois.
- Les mots de passe devraient être modifiés au moins tous les 60 jours et une personne devrait avoir utilisé au moins cinq mots de passe différents avant de pouvoir réutiliser un mot de passe antérieur.

31 La combinaison du degré d'atteinte des éléments énumérés au paragraphe précédent avec les normes en vigueur atteste du caractère approprié de la configuration des paramètres de sécurité des mots de passe.

Gestion des opérations

32 La gestion des opérations représente d'autres contrôles généraux regroupant la gestion des incidents, l'exploitation des systèmes et la continuité des services.

33 Toute déficience significative constatée dans la gestion des opérations risque moins d'avoir une incidence majeure sur la stratégie d'audit des états financiers que les contrôles mentionnés dans les paragraphes précédents. À titre d'exemple, une lacune ayant un impact sur la continuité des services informatiques n'empêche généralement pas l'utilisation de la stratégie d'audit basée sur les contrôles informatiques. Toutefois, il pourrait en être autrement pour une déficience importante sur le plan de la gestion des incidents ou de l'exploitation des systèmes, ce qui pourrait augmenter le risque de perte ou d'altération de données financières.

34 Parmi ces autres CGTI, les contrôles liés à la gestion des incidents informatiques s'avèrent cruciaux pour une organisation, compte tenu du risque important sur le plan de l'intégrité des données. Pour assurer une saine gestion de leurs incidents informatiques, les entités doivent, notamment :

- mettre en place des mécanismes d'enregistrement et d'investigation permettant une détection rapide et une résolution adéquate des anomalies, afin de s'assurer de l'intégralité et de l'intégrité des données, de même que de la poursuite ou de la reprise des activités en temps opportun ;
- présenter une reddition de comptes à la haute direction à propos des incidents jugés les plus importants.

35 L'exploitation des systèmes informatiques, en particulier les traitements en lots, affecte directement le traitement des transactions et une défaillance à cet égard menace l'ensemble des opérations de l'entité. Pour assurer la bonne marche des opérations informatiques :

- l'outil servant à établir la séquence des tâches en différé (traitements en lots) doit être sécurisé et seules les personnes autorisées doivent y avoir accès ;
- les journaux des opérations (rapports de rejets ou de fins anormales, etc.) doivent être activés et un suivi doit être effectué par une personne indépendante du personnel d'exploitation.

36 Enfin, pour ce qui est des contrôles relatifs à la continuité des services informatiques, les entités doivent principalement mettre en place les éléments suivants :

- des copies de sauvegarde des données financières et des programmes informatiques sont prises selon une fréquence appropriée et elles sont conservées ailleurs que dans l'édifice où le centre informatique se situe ;
- un plan de relève couvrant les applications informatisées importantes existe et il est testé périodiquement.

2.3 Importance de l'application des recommandations touchant les CGTI

37 La section précédente a fait ressortir les risques susceptibles de compromettre l'intégrité des données financières et qui justifient la communication de toute déficience significative dans un rapport aux responsables de la gouvernance et à la direction.

38 Le tableau 1 présente la répartition des recommandations pour les cinq sujets relatifs à la gestion des TI composant les CGTI. Nous constatons que la plupart des recommandations concernent les sujets qui risquent le plus de compromettre l'intégrité des données financières des entités auditées, soit la gestion de la maintenance des systèmes, celle des droits et des profils d'accès et, enfin, celle des paramètres de sécurité. Les déficiences qu'elles sous-tendent empêchent souvent l'utilisation d'une stratégie d'audit des états financiers basée sur les contrôles informatiques.

Tableau 1 Répartition des recommandations par sujet (gestion des technologies de l'information)

Sujets	Recommandations formulées et suivies en 2011-2012			
	Anciennes		Nouvelles	Total
	Progrès satisfaisants	Progrès insatisfaisants		
Politique et procédures de sécurité	0	0	1	1
Gestion du développement et de la maintenance des systèmes	13	6	10	29
Gestion des droits et des profils d'accès	26	25	10	61
Gestion des paramètres de sécurité	8	8	2	18
Gestion des opérations	2	1	8	11
Total	**49**	**40**	**31**	**120**

39 Les résultats de nos travaux montrent que les entités tardent à appliquer nos recommandations bien qu'elles y adhèrent.

40 Le tableau 2 présente l'historique des recommandations suivies en 2011-2012 pour la catégorie Gestion des technologies de l'information. Sur les 120 recommandations, 89 provenaient de recommandations formulées lors des années antérieures et pour lesquelles un suivi a été fait en 2011-2012. Les résultats montrent que seulement 55 % des recommandations ont été appliqués de façon satisfaisante, soit 49 sur 89. Par ailleurs, le pourcentage n'a pas augmenté de façon significative depuis les dernières années, puisqu'il était respectivement de 53 et de 54 % pour les années 2010-2011 et 2009-2010. De plus, sur les 40 recommandations dont les progrès sont toujours insatisfaisants, il est à noter que 22 d'entre elles (55 %) remontent à des années antérieures à 2009.

Tableau 2 Historique des recommandations et taux d'application (gestion des technologies de l'information)

Années d'origine	Recommandations suivies en 2011-2012			
	Progrès satisfaisants	Progrès insatisfaisants	Total	Taux d'application
2011	10	5	15	67 %
2010	8	1	9	89 %
2009	6	12	18	33 %
De 2004 à 2008	25	22	47	53 %
Total	**49**	**40**	**89**	**55 %**

2.4 Centre de services partagés du Québec

41 Une large part de nos recommandations liées à la gestion des TI concernent le Centre de services partagés du Québec (CSPQ). La diversité des systèmes et des infrastructures technologiques ainsi que l'étendue de sa clientèle peuvent expliquer cette situation. Conscient de cette problématique, le Centre prévoit entreprendre des actions concrètes pour remédier aux déficiences mentionnées dans nos rapports. Nous y porterons une attention particulière au cours des années à venir.

42 Le tableau 3 illustre que des 120 recommandations formulées et suivies auxquelles nos rapports font référence en 2011-2012, 23 entités étaient concernées. Le CSPQ était visé par 46 de ces recommandations, soit plus du tiers. De plus, parmi les 40 recommandations dont les progrès ont été jugés insatisfaisants, nous constatons que 25 concernent le CSPQ. Ces recommandations datent de 2008 et de 2009. Enfin, des 31 nouvelles recommandations formulées en 2011-2012 à l'endroit de 9 entités, le CSPQ en compte 11 d'entre elles. Ces recommandations concernent l'exercice du CSPQ terminé le 31 mars 2011.

Tableau 3 Situation du CSPQ par rapport aux recommandations (gestion des technologies de l'information)

	Ensemble des 23 entités auditées	CSPQ Au 31 mars 2011
2005 à 2009	34	25
2010 et 2011	6	–
Progrès insatisfaisants	**40**	**25**
Progrès satisfaisants	49	10
Anciennes recommandations	**89**	**35**
Nouvelles recommandations	31	11
Nombre de recommandations	120	46

43 Les résultats des travaux d'audit que nous avons effectués auprès du CSPQ pour l'exercice terminé le 31 mars 2012 révèlent que le faible taux d'application de nos recommandations se maintient. En effet, 6 des 25 anciennes recommandations datant de 2008 et de 2009, dont les progrès avaient été jugés insatisfaisants et aucune des 11 recommandations relatives à l'exercice terminé le 31 mars 2011, ont été appliquées de manière satisfaisante, ce qui représente un taux d'application de 17 % (6 sur 36).

Création du Centre de services partagés du Québec

44 Le CSPQ a démarré officiellement ses activités le 6 décembre 2005 à la suite de l'adoption de la *Loi sur le Centre de services partagés du Québec* le 11 mai 2005. Le CSPQ est formé du regroupement d'une dizaine d'organismes de services gouvernementaux, dont les principaux sont : Fourniture et ameublement du Québec, la Direction générale des acquisitions, la Direction

générale des technologies de l'information et des communications et la Direction générale des solutions d'affaires en gestion intégrée des ressources. Le Centre a pour mission de fournir aux organismes publics les biens et les services administratifs dont ils ont besoin dans l'exercice de leurs fonctions, notamment en matière de ressources humaines, financières, matérielles et informationnelles.

45 À sa création, le CSPQ comprenait une multitude de systèmes informatiques liés à sa mission, dont 5 systèmes comptables, 16 systèmes de facturation, 12 systèmes servant à la gestion de l'encaisse, des immobilisations et des projets en cours, et 17 systèmes pour la gestion des stocks et des acquisitions de biens, l'ensemble supporté par des infrastructures technologiques diversifiées. Le CSPQ s'est donc trouvé devant un défi majeur d'harmonisation aussi bien sur le plan de la gestion des TI que sur celui des ressources humaines, chaque organisme regroupé ayant ses propres méthodes de travail.

Plan d'action préconisé par le Centre de services partagés du Québec

46 En réponse à notre intervention, une décision du comité de direction du CSPQ a été prise le 10 décembre 2012. Celle-ci consiste à mettre en place un registre du suivi des actions prises par le Centre pour donner suite à chacune des recommandations que nous leur avons formulées en matière de gestion des TI et dont les progrès demeurent toujours insatisfaisants en 2012, de même que pour toute nouvelle recommandation qui leur sera adressée. On y prévoit qu'un suivi serré sera fait et, à cette fin, le registre sera mis à jour trimestriellement et présenté au comité de direction de même qu'au comité de vérification afin d'en évaluer le taux d'avancement.

47 En janvier 2013, le registre a effectivement été produit. Il comprend, pour chacune des recommandations, l'état de la situation, les actions qui seront prises, le nom du responsable et l'échéancier de mise en place. Selon les échéanciers inscrits au registre, 20 des 30 recommandations qui y figurent devraient avoir un statut défini comme terminé au 31 décembre 2013. En y ajoutant les 6 recommandations jugées satisfaisantes dans notre rapport du 31 mars 2012, 72 % de nos recommandations devraient être appliquées d'ici la fin 2013. Des 10 recommandations dont l'application n'est pas prévue en 2013, 5 concernent la mise en place d'un plan de relève assurant la continuité des opérations. Dans ce dernier cas, un mandat d'évaluation des besoins et d'analyses de leur impact éventuel est en cours, ce qui déterminera l'échéancier de mise en œuvre. Pour ce qui est des autres recommandations, certaines analyses d'impact sont également en cours. Nous validerons les actions prises au cours des prochains audits financiers et nous invitons le CSPQ à mener à terme les actions qu'il a entreprises.

Commentaires de l'entité

Le Centre de services partagés du Québec a eu l'occasion de transmettre ses commentaires, qui sont reproduits dans la présente section.

Commentaires du Centre de services partagés du Québec

« Le Centre de services partagés du Québec (CSPQ) est soucieux de donner suite de manière satisfaisante aux recommandations formulées par le Vérificateur général du Québec (VGQ). Cette volonté s'est exprimée par une démarche rigoureuse qui exige que toutes les actions et les moyens soient mis en œuvre afin de s'assurer du suivi des progrès réalisés. Cette démarche mise en place en décembre 2012 prévoit un registre de suivi trimestriel qui implique tous les secteurs concernés, une présentation au comité de direction pour s'assurer de l'état d'avancement des travaux et déposé au conseil d'administration.

« De cette façon, la majorité des recommandations seront appliquées au 31 décembre 2013. Le CSPQ s'est doté d'un processus qui lui permettra de répondre adéquatement au suivi de toutes nouvelles recommandations du VGQ. »

Sigles

Sigles

CGTI	Contrôles généraux des technologies de l'information	**TI**	Technologie de l'information
CSPQ	Centre de services partagés du Québec	**VGQ**	Vérificateur général du Québec