

CHAPITRE

9

Contrôles généraux des technologies de l'information

Mise en contexte

- Un portrait des rapports aux responsables de la gouvernance et à la direction est dressé pour une troisième année consécutive au chapitre 9 du présent Tome.
- 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.
- Ce chapitre présente les principaux éléments ressortant des travaux d'audit des contrôles généraux des technologies de l'information (CGTI) réalisés au VGQ dans le contexte de nos mandats d'audit financier.

Importance des CGTI dans le processus de préparation des états financiers

- Les CGTI représentent un des fondements du contrôle interne de l'entité et interviennent tout au long du processus de production des états financiers.
- La fiabilité du fonctionnement des CGTI garantit le niveau de confiance acceptable accordée à l'ensemble des contrôles liés aux applications informatiques, notamment celles de nature financière.
- Les CGTI comprennent un ensemble de politiques et de procédures encadrant la sécurité de l'information et les processus relatifs à la gestion des TI.

CGTI et sécurité de l'information

- Lors de l'audit des CGTI, nous portons une attention particulière aux contrôles assurant l'intégrité des données financières.
- La sécurité de l'information s'évalue selon trois objectifs
 - **Disponibilité** : garantir que les systèmes sont accessibles au moment voulu et fonctionnent sans faille durant les périodes d'utilisation prévues
 - **Intégrité** : prévenir que les données ne soient pas altérées ou détruites de façon fortuite ou volontaire
 - **Confidentialité** : assurer que seules les personnes autorisées peuvent accéder en mode lecture à des fins de consultation aux informations qui leur sont destinées

Approche d'audit des CGTI adoptée au VGQ

NOTRE APPROCHE

- Conforme aux Normes d'audit généralement reconnues, incluant les NCA et s'appuie sur des référentiels
- Vigie avec les grands cabinets d'experts-comptables
- Basée sur une méthodologie couvrant cinq sujets
 - 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

Approche d'audit des CGTI adoptée au VGQ (suite)

- Les contrôles liés 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 ont un impact majeur sur l'intégrité des données financières.
- Toute déficience significative de l'un des contrôles clés relatifs à ces CGTI
 - empêche souvent l'utilisation d'une stratégie d'audit des états financiers basée sur les contrôles informatiques
 - entraîne une recommandation dans un rapport aux responsables de la gouvernance et à la direction

Approche d'audit des CGTI adoptée au VGQ (suite)

EXEMPLES DE PROCESSUS ADÉQUATS

- Pour la gestion du développement et de la maintenance des systèmes
 - Essais des modifications aux programmes effectués dans un environnement distinct de celui de la production
 - Autorisation du responsable des utilisateurs avant la mise en production des programmes
- Pour la gestion des droits et des profils d'accès
 - Autorisation formelle du gestionnaire avant l'octroi des droits d'accès lors de l'arrivée d'un nouvel employé
 - Retrait en temps opportun des droits d'accès lors du départ d'un employé

Approche d'audit des CGTI adoptée au VGQ (suite)

Exemples de risques liés à une déficience significative

- Gestion du développement et de la maintenance des systèmes
 - Risque que des modifications non autorisées soient apportées aux programmes ou aux données financières
 - Risque que des modifications nécessaires ne soient pas réalisées ou ne soient pas effectuées adéquatement
- Gestion des accès
 - Risque d'accès non autorisé aux données financières pouvant conduire
 - à leur destruction
 - à des modifications inappropriées, dont l'enregistrement d'opérations non autorisées ou inexistantes

Importance de l'application des recommandations touchant les CGTI

- La plupart des 120 recommandations formulées et suivies en 2011-2012 concernent les sujets qui risquent le plus de compromettre l'intégrité des données financières des entités auditées, soit
 - la gestion du développement et de la maintenance des systèmes (29 soit 24 %)
 - la gestion des droits et des profils d'accès (61 soit 51 %)
 - la gestion des paramètres de sécurité (18 soit 15 %)
- Les entités tardent à appliquer nos recommandations
 - Seulement 49 des 89 recommandations formulées lors des années antérieures ont été appliquées (55 %)
 - 22 des 40 recommandations ayant un progrès insatisfaisant remonte à des années antérieures à 2009 (55 %)

Centre de services partagés du Québec (CSPQ)

Situation du CSPQ

- Une large part de nos recommandations liées à la gestion des TI concernent le CSPQ, comme le démontre le tableau suivant.

	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

Centre de services partagés du Québec (suite)

Plan d'action préconisé par le CSPQ

- Le CSPQ a entrepris des actions concrètes pour remédier à cette situation
 - Registre de suivi des actions prises pour donner suite à nos recommandations produit en janvier 2013
 - Mise à jour trimestrielle du registre qui sera déposé au comité de direction et au comité de vérification
- Selon les échéanciers prévus au registre
 - 72 % de nos recommandations devraient être appliquées d'ici le 31 décembre 2013.