GUIDE

À L'INTENTION DES ENTITÉS AUDITÉES

AUDIT DES CONTRÔLES GÉNÉRAUX INFORMATIQUES DANS LE CADRE DE L'AUDIT DES ÉTATS FINANCIERS

VGQ
Vérificateur général du Québec

Cette publication
est rédigée par le

VGQ
Vérificateur général du Québec

Québec
575, rue Jacques-Parizeau, bureau 300
Québec (Québec) G1R 2G4
Téléphone : 418 691-5900

Montréal
770, rue Sherbrooke Ouest, bureau 1920
Montréal (Québec) H3A 1G1
Téléphone : 514 873-4184

Internet
Courriel : verificateur.general@vgq.qc.ca
Site Web : www.vgq.qc.ca

Suivez-nous sur les médias sociaux

Vérificateur général du Québec, février 2025.

TABLE DES MATIÈRES

1. OBJECTIF DU GUIDE

DANS LE CADRE DE SES TRAVAUX, LE VÉRIFICATEUR GÉNÉRAL DU QUÉBEC S'EFFORCE DE PROMOUVOIR LE RESPECT ET LA CONFIANCE DANS SES RELATIONS AVEC L'ENTITÉ[1] TOUT EN MAINTENANT SON INDÉPENDANCE ET EN FAISANT PREUVE DE RIGUEUR ET D'OBJECTIVITÉ.

Le présent guide a été rédigé à l'intention de la **direction des technologies de l'information** de l'entité auditée. Il présente le déroulement de l'audit des contrôles généraux informatiques (CGI) qui a lieu dans le cadre de l'audit des états financiers annuels de l'entité.

Ce document présente le contexte et les assises d'intervention du Vérificateur général. Il explique chacune des étapes de la réalisation des travaux sur les CGI et la participation qui est attendue de la direction des technologies de l'information, et il décrit les principaux CGI audités. Enfin, il informe sur les rapports publiés et les suites de l'audit. Les différences entre l'audit des CGI dans le cadre de l'audit des états financiers et l'audit de performance lié aux technologies de l'information sont présentées en annexe.

1. Il est à noter que, dans le présent guide, le terme générique « entité » est utilisé pour désigner les ministères et les organismes publics.

2. MISE EN CONTEXTE

Pour répondre aux risques découlant du recours aux technologies de l'information et assurer un fonctionnement efficace, continu et intègre des applications et de l'infrastructure technologique, l'entité doit mettre en place un ensemble de contrôles internes, y compris des contrôles généraux informatiques (CGI).

Des CGI fiables assurent le maintien d'un niveau adéquat de sécurité de l'information et représentent un des piliers du contrôle interne. Sans l'assurance que procure un environnement de CGI fiable, il devient plus risqué de se fier aux applications et à l'infrastructure technologique nécessaires à la production de l'information financière.

CGI

Contrôles afférents aux processus informatiques de l'entité qui contribuent à assurer le bon fonctionnement continu de l'environnement informatique, notamment le maintien du fonctionnement efficace des contrôles du traitement de l'information et l'intégrité des informations se trouvant dans le système d'information de l'entité[2].

L'audit des CGI qui a lieu dans le cadre de l'audit des états financiers concerne les systèmes d'information qui ont un impact sur la préparation des états financiers. Par le fait même, les autres systèmes liés à la mission de l'entité sont la plupart du temps exclus de la portée des travaux d'audit.

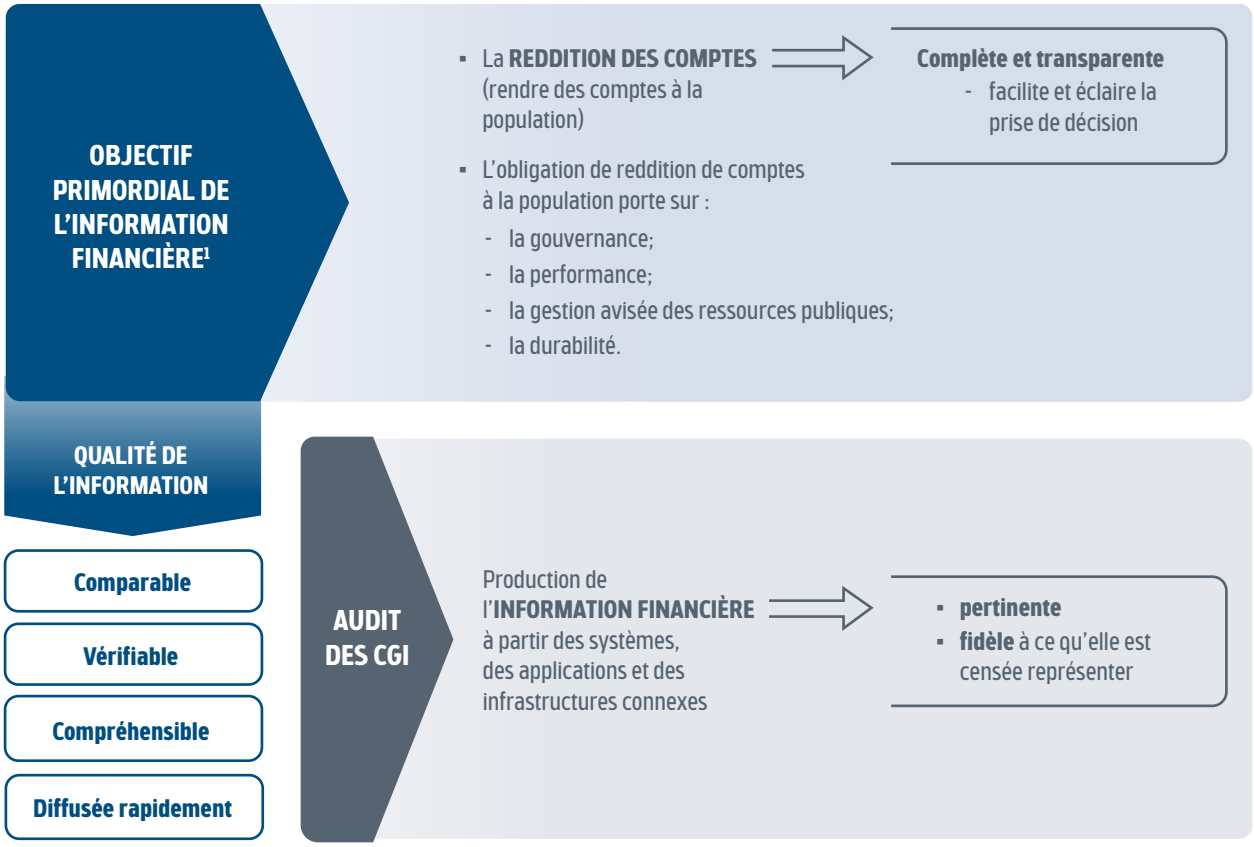
Dans ce contexte, l'auditeur informatique travaille en soutien à l'auditeur des états financiers qui, lui, a la responsabilité, selon les Normes canadiennes d'audit, de déterminer les risques d'anomalies significatives découlant du recours aux technologies de l'information lors de la préparation des états financiers. Rappelons que l'objectif de l'audit des états financiers est de délivrer une opinion en obtenant l'assurance raisonnable que, pris dans leur ensemble, ils sont exempts d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs[3] (figure 1).

FIGURE 1 But de l'audit des CGI dans le cadre de l'audit des états financiers

2. Cette définition est tirée de la norme canadienne d'audit 315.12d *Identification et évaluation des risques d'anomalies significatives* (décembre 2021).
3. Cette définition est tirée de la norme canadienne d'audit 200 *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux Normes canadiennes d'audit*.

Ainsi, l'audit des CGI vise à s'assurer que l'usage de l'informatique ne présente pas de risque résiduel significatif. Il permet donc que l'entité puisse fournir l'assurance raisonnable que son information financière est pertinente pour les utilisateurs des états financiers et qu'elle reflète une image fidèle de ce qu'elle est censée représenter (figure 2).

FIGURE 2 Objectif et qualités recherchées de l'information financière



1. Définition tirée du Cadre conceptuel de l'information financière dans le secteur public publié dans le *Manuel de CPA Canada pour le secteur public*.

Dans le cadre des travaux d'audit financier, nous acquérons une compréhension des CGI et réalisons des travaux afin de concevoir des procédures pertinentes appropriées aux circonstances et non dans le but d'exprimer une opinion sur l'efficacité des CGI.

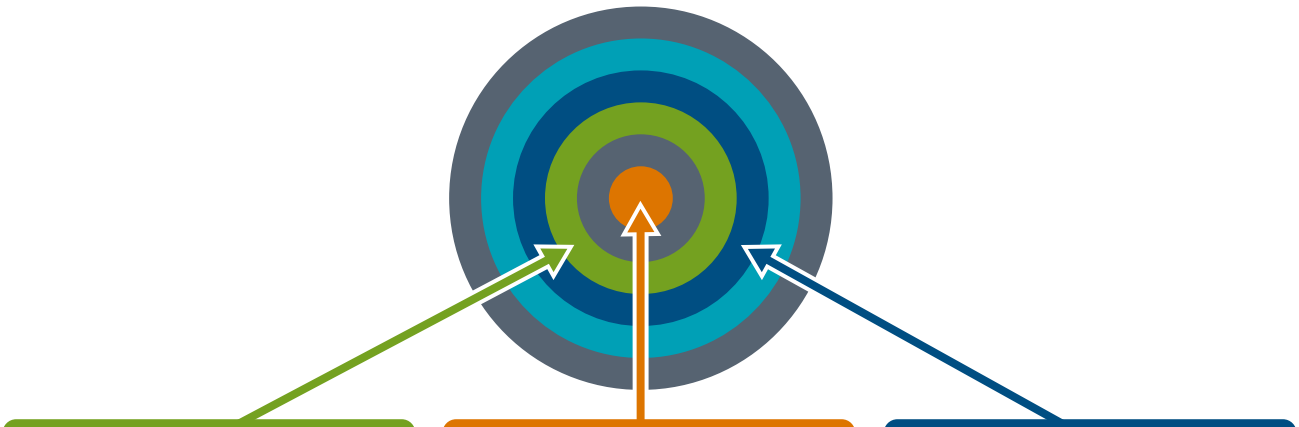
3. ASSISES D'INTERVENTION DU VÉRIFICATEUR GÉNÉRAL

3.1 Principes de sécurité de l'information

La disponibilité, l'intégrité et la confidentialité (DIC) sont les principes fondamentaux de sécurité de l'information. Lors de l'audit des CGI dans le cadre de l'audit des états financiers, le Vérificateur général porte une attention particulière aux CGI assurant **l'intégrité** des données pour les systèmes pertinents à cet égard.

La figure 3 montre le niveau d'importance du respect des chacun des trois principes de sécurité de l'information dans le cadre de l'audit des états financiers.

FIGURE 3 Niveau d'importance du respect des principes de sécurité de l'information dans le cadre de l'audit des états financiers



DISPONIBILITÉ

- S'assurer que les systèmes sont accessibles au moment voulu pour les personnes autorisées.

  Les CGI assurant la disponibilité des données font seulement l'objet de travaux d'audit sommaires, puisque la non-disponibilité a normalement peu d'impact sur la fiabilité des données financières. L'auditeur n'effectue aucun test exhaustif quant à l'efficacité du plan de reprise informatique, outre de s'assurer qu'un tel plan existe et que des tests sont planifiés et effectués annuellement. Des travaux minimums sont également effectués sur la procédure de sauvegarde. Des travaux plus étendus peuvent être requis lors d'une perte importante de données (ex. : cyberattaques).

INTÉGRITÉ

- S'assurer que les données ne sont pas altérées ni détruites de façon fortuite ou volontaire lors de leur traitement, de leur conservation ou de leur transmission, afin de garantir :
  - leur exhaustivité;
  - leur exactitude;
  - leur validité.

  Les CGI assurant l'intégrité des données et des traitements sont audités, puisque la fiabilité des données inscrites dans les états financiers en dépend.

CONFIDENTIALITÉ

- S'assurer que seules les personnes autorisées peuvent accéder à des informations confidentielles lorsqu'elles sont nécessaires à l'exercice de leurs fonctions.

  Il n'y a pas de travaux sur les CGI assurant la protection des données confidentielles tant qu'aucun incident ne survient, puisque le risque de fuite de telles données ne représente habituellement pas un risque d'altération des données financières. Lors d'un incident, l'auditeur doit cependant évaluer son impact sur les états financiers et le risque d'anomalies significatives.

3.2 Normes d'audit financier en lien avec l'audit des CGI

L'audit financier est assujetti aux Normes canadiennes d'audit (NCA). Les principales étapes d'un audit des états financiers selon les NCA qui requièrent des travaux d'audit des CGI sont présentés dans la figure 4.

FIGURE 4 Principales étapes de l'audit des états financiers selon les NCA qui requièrent l'audit de CGI

Étape 1	▪ Acceptation du mandat (NCA 210)
Étape 2	▪ Prise de connaissance de l'entité et de son environnement interne (NCA 200 et NCA 315) ▪ Identification des risques d'anomalies significatives[1] en se fondant sur : - la compréhension du système de contrôle interne - les risques connexes découlant du recours à l'informatique - les contrôles généraux informatiques visant à répondre à ces risques ▪ Identification des applications informatiques et des autres aspects de l'environnement informatique ainsi que de son infrastructure et des processus ▪ Obtention de l'assurance raisonnable que les états financiers pris dans leur ensemble ne comportent pas d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs (NCA 240) ▪ Acquisition de la compréhension de la nature des prestations fournies par la société de services (impartiteur informatique), de leur incidence sur les contrôles internes de l'entité et du degré d'interaction entre les activités de la société de services et celles de l'entité utilisatrice (NCA 402)
Étape 3	▪ Conception de procédures d'audit en réponse aux risques évalués (NCA 330) ▪ Conception et mise en place de tests sur les contrôles dans le cas où les procédures de corroboration[2] ne peuvent fournir à elles seules des éléments probants suffisants et appropriés (NCA 330)
Étape 4	▪ Synthèse du mandat et rédaction du rapport de l'auditeur indépendant concernant les états financiers (NCA 700)

1. Il s'agit de déterminer les risques que les états financiers puissent comporter des anomalies significatives avant de commencer l'audit.
2. Il s'agit de procédures d'audit conçues pour détecter des anomalies significatives au niveau des assertions contenues dans les états financiers.

3.3 Référentiels en technologies de l'information

Pour mener à bien son mandat, l'auditeur informatique :

- s'appuie sur des référentiels reconnus au Canada comme dans le monde, qui forment un ensemble structuré de bonnes pratiques s'adressant à toutes les entités, tant gouvernementales que privées;
- s'assure que les bonnes pratiques présentées dans ces référentiels sont adaptées aux objectifs et aux risques du recours à l'informatique de l'entité auditée;
- se base notamment sur les Normes canadiennes d'audit, dont la norme intitulée *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives* (NCA 315).

Voici des exemples de référentiels internationaux pris en considération :

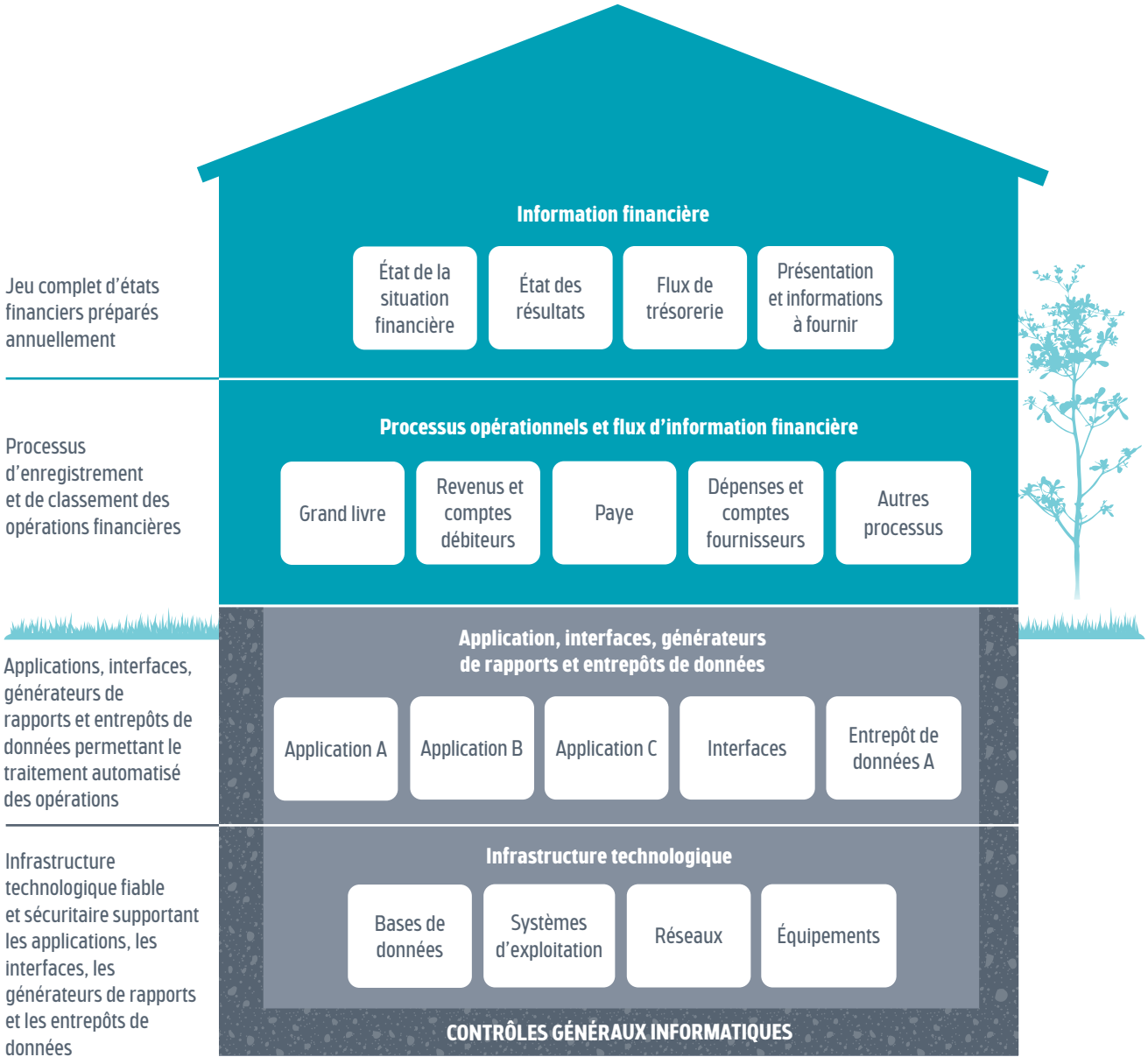
- Objectifs de contrôle de l'information et des technologies associées **(COBIT)**[4]
- Organisation internationale de normalisation **(ISO)**[5], principalement la norme ISO/IEC 27002 Technologies de l'information — *Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*
- Institut national des normes et de la technologie **(NIST)**[6], principalement le cadre de sécurité NIST 800-53 *Contrôles de sécurité et de confidentialité pour les systèmes d'information et les entités*.

4. D'origine américaine, COBIT est un référentiel de bonnes pratiques en matière d'audit informatique et de gouvernance des systèmes d'information.
5. L'ISO est une organisation internationale de normalisation composée de représentants d'organisations nationales de normalisation de nombreux pays. Elle produit des normes internationales utiles aux organisations industrielles et économiques de tous types, et aux gouvernements.
6. La NIST est une agence du U. S. Department of Commerce. Elle a pour but de promouvoir l'économie en développant de concert avec l'industrie des technologies, la métrologie et des normes.

3.4 Systèmes d'information visés par l'audit des CGI

Comme l'illustre la figure 5, l'audit concerne les CGI à l'égard de l'infrastructure technologique, des applications et leurs interfaces, des générateurs de rapports et des entrepôts de données qui sont à la source de la préparation des états financiers. L'auditeur détermine les processus opérationnels, les applications et infrastructures à auditer en fonction de leur utilité lors de la préparation des états financiers.

FIGURE 5 Environnement des CGI audités dans le cadre de l'audit des états financiers



3.5 Deux stratégies d'audit financier

En audit des états financiers, il existe deux principales stratégies : l'une axée sur les contrôles et l'autre dite corroborative. L'auditeur financier détermine la stratégie qu'il juge la plus efficiente et efficace selon sa compréhension de l'environnement informatique de l'entité acquise lors de la planification de l'audit. Ce choix est notamment appuyé par son appréciation des risques, le niveau d'informatisation des processus, la complexité des systèmes en place et le volume de transactions de l'entité.

Il faut noter que les deux stratégies mettent en lumière l'importance de la fiabilité des CGI, et par le fait même l'impact de ceux-ci sur la qualité de l'information financière fournie entité. Elles montrent aussi l'apport des tests effectués pendant l'audit pour permettre à l'entité de connaître les déficiences de ses CGI, le cas échéant.

Les principales différences entre ces deux stratégies d'audit des états financiers de l'entité et leur impact respectif sur l'audit des CGI sont présentées ci-après.

	STRATÉGIE AXÉE SUR LES CONTRÔLES	STRATÉGIE CORROBORATIVE
Objectif	L'auditeur financier compte s'appuyer sur des contrôles et des traitements informatiques pour obtenir l'assurance raisonnable que les données financières sont fiables.	L'auditeur financier ne s'appuie pas sur les contrôles informatiques pour formuler une opinion sur les états financiers.
Travaux d'audit des CGI	L'auditeur informatique évalue les risques du recours à l'informatique. Il teste : ▪ la conception et la mise en place des CGI à un moment donné, ▪ le fonctionnement efficace des CGI durant l'exercice financier qui est habituellement de 12 mois, s'il y a lieu.	L'auditeur informatique évalue les risques du recours à l'informatique. Il teste la conception et la mise en place des CGI à un moment donné.
Impact de l'audit des CGI sur l'audit des états financiers	Lorsque l'auditeur informatique conclut que les CGI sont fiables, l'auditeur financier peut tester une seule fois les traitements et les contrôles automatisés au sein des applications afin d'obtenir l'assurance raisonnable que l'information financière est fiable pour la période auditée. Cette stratégie permet de réduire la quantité des travaux de corroboration de l'auditeur financier. Elle devient incontournable lorsque les procédures de corroboration ne peuvent fournir, à elles seules, des éléments probants suffisants et appropriés, notamment dans le cas d'un système hautement informatisé et utilisé pour nombreuses transactions.	L'auditeur financier évalue l'impact des CGI déficients sur la fiabilité des états financiers et réalise les procédures de corroboration.
Sollicitation de la direction des technologies de l'information	Très sollicitée	Peu à moyennement sollicitée

4. DÉROULEMENT DE L'AUDIT DES CGI

Les étapes de l'audit des CGI dans le cadre de l'audit des états financiers et la participation attendue de la direction des technologies de l'information à chacune de ces étapes sont présentées dans la figure 6.

FIGURE 6 Étapes de l'audit des CGI dans le cadre de l'audit des états financiers et participation attendue de la direction des TI

1 PREMIERS CONTACTS

- Participer à une rencontre initiale avec l'auditeur informatique du Vérificateur général
- Nommer un interlocuteur principal au sein de la direction des TI

2 PLANIFICATION

Répondre aux demandes du Vérificateur général concernant

- les activités et composantes de l'environnement informatique
- la description des processus des CGI

3 TRAVAUX D'AUDIT

Fournir les éléments probants demandés

4 LETTRE D'OBSERVATIONS OU RAPPORT AUX RESPONSABLES DE LA GOUVERNANCE ET À LA DIRECTION

- Prendre connaissance des déficiences des CGI et/ou des recommandations
- Adhérer aux recommandations, s'il y a lieu
- Rédiger des commentaires officiels, le cas échéant
- Produire un plan d'action, s'il y a lieu

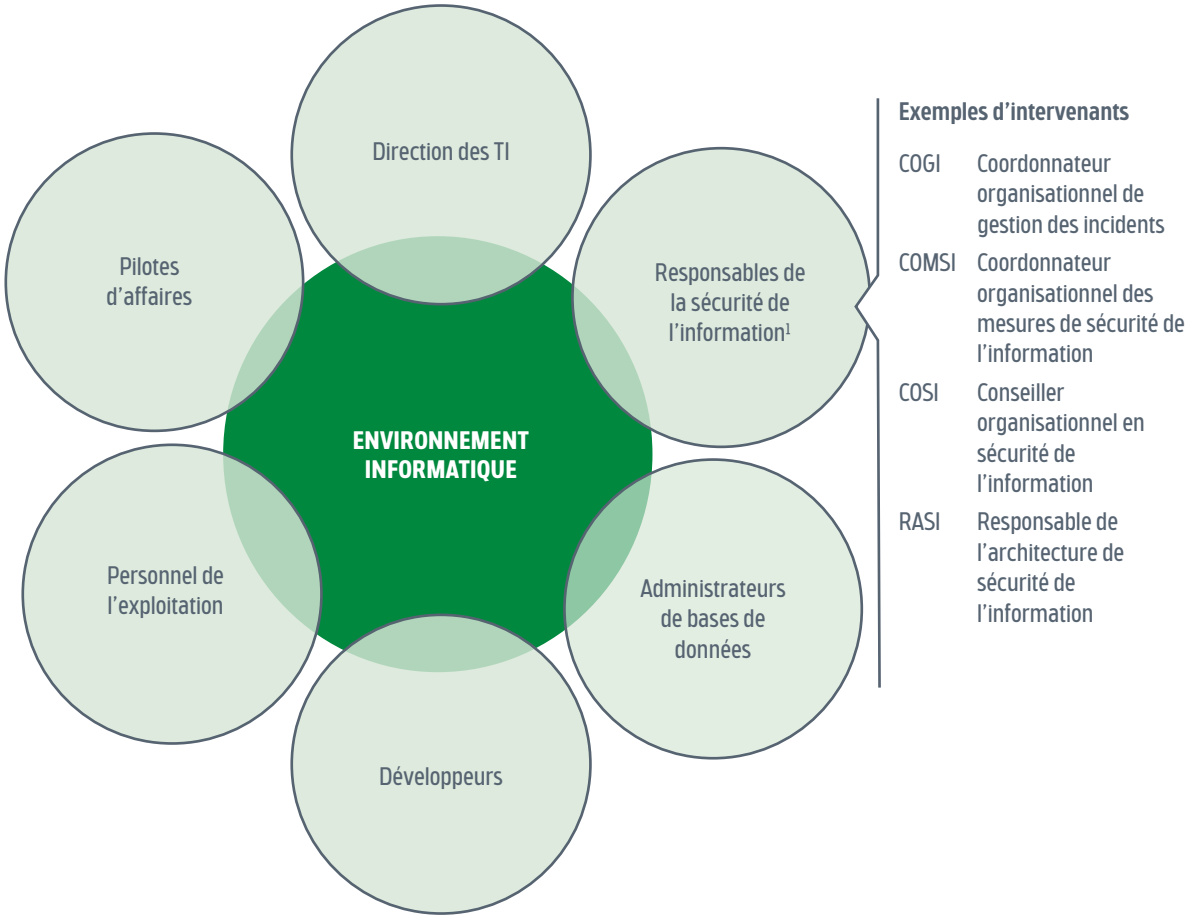
5 SUITES DE L'AUDIT

- Le Vérificateur général présente les résultats de l'audit au comité d'audit interne de l'entité.
- L'entité participe à un suivi de son plan d'action.

Il est primordial que l'entité auditée prévoie dans sa planification annuelle le temps nécessaire pour répondre aux demandes de l'auditeur afin qu'il puisse fournir les résultats de ses travaux dans les délais attendu.

Les principaux intervenants de la direction des technologies de l'information qui peuvent être sollicités pendant l'audit pour fournir l'information sur les risques, les CGI des processus automatisés et les informations générées qui sont utiles dans le cadre de l'audit des états financiers sont présentés dans la figure 7. Le ministère de la Cybersécurité et du Numérique peut aussi être sollicité pour nous fournir certaines informations.

FIGURE 7 Principaux intervenants en TI pouvant être sollicités pendant l'audit des CGI



1. Les tâches respectives des intervenants sont définies dans le document *Cadre de gestion gouvernemental : Sécurité de l'information*. Cette liste de responsables de la sécurité de l'information n'est pas exhaustive.

4.1 Premiers contacts

L'auditeur informatique tient généralement une première réunion avec les représentants de la direction des technologies de l'information pour présenter le déroulement de l'audit des CGI et discuter du mode de fonctionnement souhaité. L'auditeur des états financiers tient pour sa part une rencontre d'information avec la haute direction, les membres du comité d'audit ou du conseil d'administration de l'entité, le cas échéant, pour présenter le déroulement de l'audit des états financiers.

La direction des technologies de l'information est invitée à nommer un responsable qui servira d'interlocuteur principal lors des travaux d'audit des CGI. Cette personne a pour rôle de coordonner et de faciliter l'exécution des travaux, soit de préparer la venue de l'équipe d'audit du Vérificateur général (ex. : attribuer les droits d'accès), de désigner les personnes pouvant fournir l'information demandée, etc.

4.2 Planification

Lors de la planification, l'auditeur financier et l'auditeur informatique acquièrent une connaissance appropriée des activités de l'entité auditée en vue de déterminer les éléments précis qui feront l'objet des travaux (figure 8).

FIGURE 8 Procédés utilisés pendant la planification de l'audit

L'information nécessaire à la compréhension de l'audit financier est consignée par l'auditeur des états financiers dans un plan d'audit qui est communiqué à la haute direction et au comité d'audit de l'entité. Ce plan comporte principalement l'information suivante :

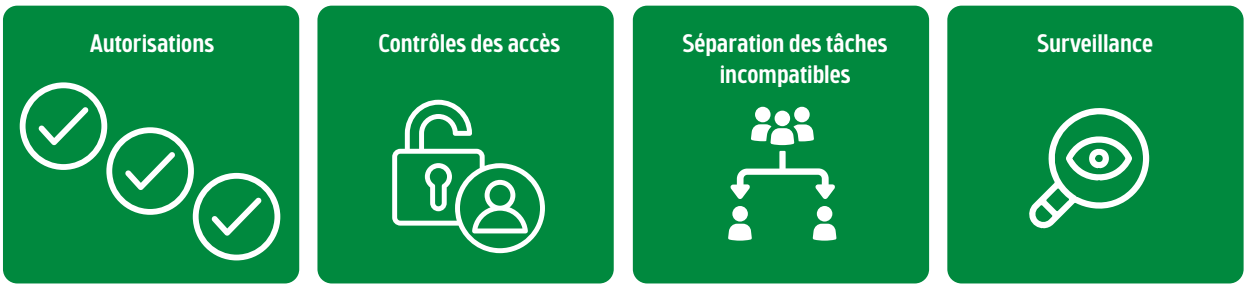
- la présentation des membres de l'équipe d'audit;
- le mandat et les conditions de la mission d'audit financier;
- le seuil de signification utilisé pour l'audit;
- les risques significatifs déterminés et les procédures prévues pour y répondre;
- la stratégie d'audit prévue (axée sur les contrôles ou corroborative);
- les responsabilités clés de la gouvernance et de la direction de l'entité ainsi que celles du Vérificateur général.

L'auditeur informatique communique pour sa part l'information suivante à la direction des technologies de l'information lors de la première réunion :

- les membres de l'équipe d'audit;
- la portée des travaux d'audit sur les CGI (ex. : applications et CGI visés);
- la période couverte par l'audit;
- les dates clés.

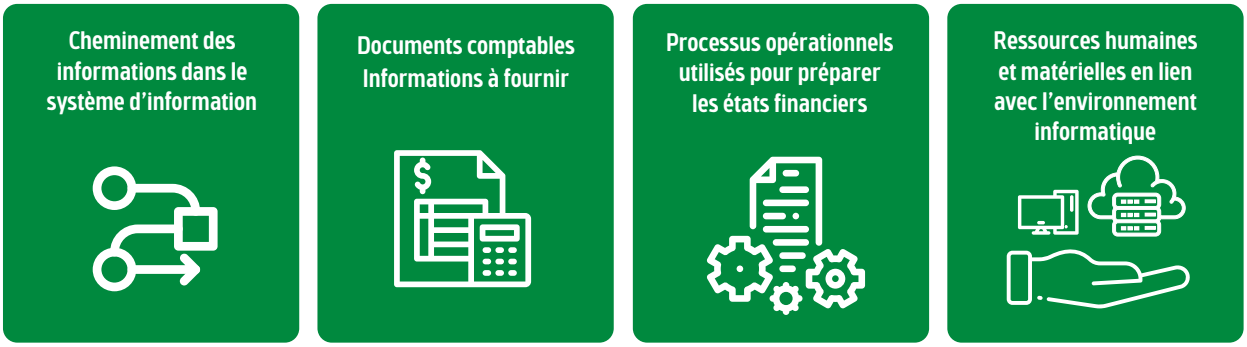
Avant de commencer l'audit, l'auditeur informatique analyse l'environnement informatique afin de prendre connaissance des activités de contrôle ayant un impact sur la fiabilité des données financières (figure 9) ainsi que de la documentation probante à l'appui de ces activités.

FIGURE 9 Exemples d'activités de contrôle à comprendre avant de commencer l'audit



L'auditeur doit aussi acquérir une bonne connaissance des éléments présentés dans la figure 10. L'entité doit lui fournir les informations sur les changements importants survenus au cours de l'exercice financier audité (ex. : nouveau système informatique, modification du processus des opérations financières, conversion de données) afin qu'il puisse évaluer les risques associés à ces changements.

FIGURE 10 Exemples d'éléments d'un système d'information à comprendre avant de commencer l'audit

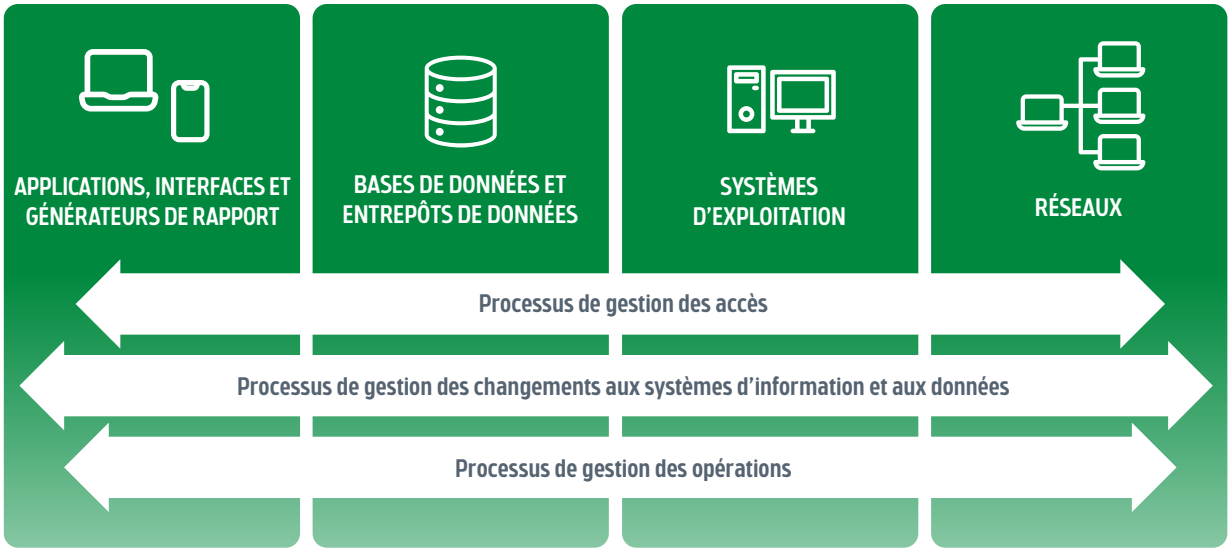


4.3 Travaux d'audit

L'audit des CGI est basé sur une méthodologie qui regroupe un ensemble de procédures d'audit appliquées à l'environnement informatique. Comme l'illustre la figure 11, l'audit couvre trois principaux processus informatiques :

- la gestion des accès;
- la gestion des changements aux systèmes d'information et aux données;
- la gestion des opérations.

FIGURE 11 Processus informatiques[1] audités dans le cadre de l'audit des états financiers



1. Des CGI sont habituellement en place dans l'ensemble des systèmes d'information de l'entité.

Ce sont les CGI des processus de gestion des accès et de gestion des changements aux systèmes et aux données qui assurent principalement **l'intégrité** des données financières. Toute déficience significative de ces CGI représente un risque important pouvant souvent empêcher l'utilisation d'une stratégie d'audit axée sur les contrôles et donc changer la stratégie d'audit. De plus, une déficience dans l'un des CGI de ces processus fait habituellement l'objet de recommandations (voir la section 5).

4.3.1 Politiques, directives et procédures relatives aux TI

La direction doit témoigner d'une préoccupation constante quant à l'ensemble de son contrôle interne, notamment en ce qui concerne la gestion des risques et les contrôles liés aux technologies de l'information. La mise en place et l'application de politiques et de procédures est l'un des éléments importants, car ces dernières indiquent les principes directeurs et établissent les rôles et les responsabilités des principaux intervenants en matière de sécurité de l'information.

L'auditeur informatique s'assure que l'entité s'est dotée de telles mesures d'encadrement et que celles-ci sont communiquées à tout le personnel concerné. Le maintien d'activités de surveillance et de reddition de comptes, comme la mise en place d'un comité de sécurité, est également pris en compte.

4.3.2 Audit des CGI de la gestion des accès

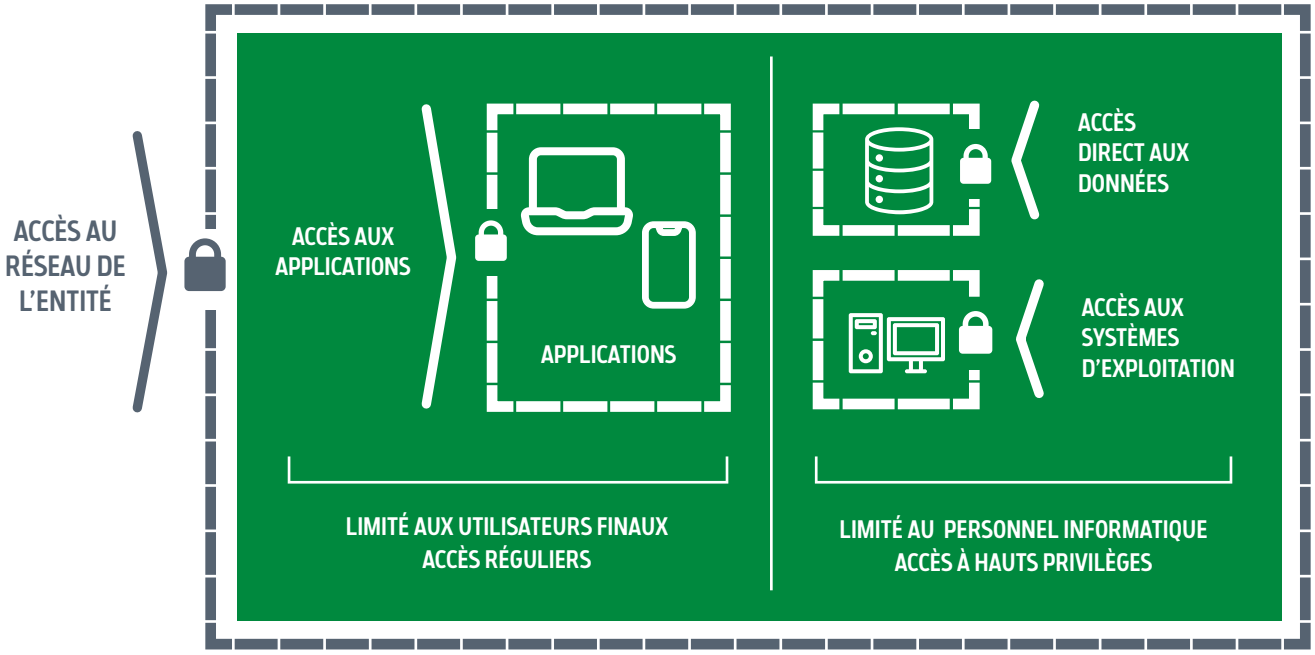
L'audit des CGI de la gestion des accès regroupe :

- les contrôles des accès aux systèmes d'information et aux données considérés comme cruciaux pour assurer l'intégrité des données et des traitements;
- les contrôles des accès physiques à l'infrastructure technologique.

CGI des accès logiques

Il y a différentes façons d'accéder aux systèmes d'information et aux données. Chacun des points d'accès doit être audité selon le niveau de risque qui lui est associé. La figure 12 présente un exemple de points d'accès aux systèmes d'information et aux données que l'auditeur doit comprendre afin d'évaluer le risque associé à l'usage de l'informatique et le besoin d'audit.

FIGURE 12 Exemples de points d'accès aux systèmes d'information et aux données



Les déficiences de contrôle significatives qui concernent la gestion des accès augmentent le risque d'accès non autorisé aux données et aux traitements des applications ciblées par l'audit. Ces déficiences peuvent conduire à la destruction ou à la modification inappropriée de données, y compris à l'enregistrement d'opérations non autorisées, et ce, par erreur ou de façon volontaire. Une déficience de contrôle concernant la gestion des accès peut prendre la forme d'un processus d'authentification non suffisamment robuste, d'un accès sans autorisation ou d'un droit d'accès qui n'a pas été révoqué en temps opportun.

L'audit des CGI des accès logiques vise principalement :

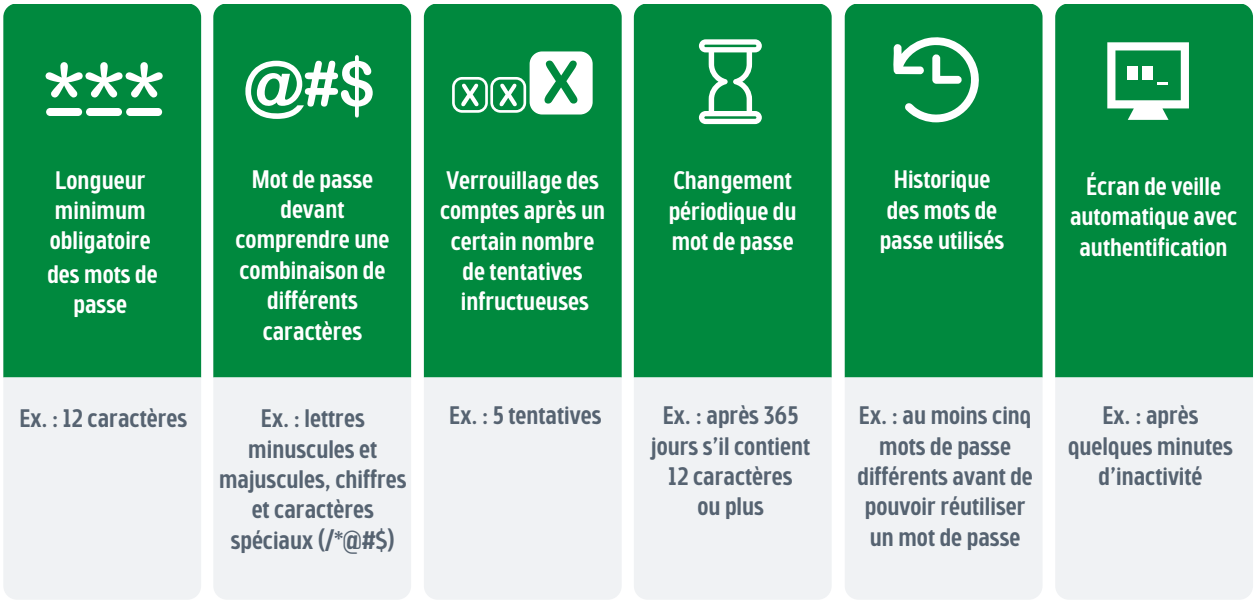
- les paramètres d'authentification;
- les processus d'attribution, de modification et de révocation des droits d'accès.

Paramètres d'authentification

L'utilisation de mots de passe est le mécanisme le plus couramment utilisé pour authentifier un individu qui veut accéder aux systèmes d'information. D'autres mécanismes sont également nécessaires, telle l'authentification multifacteur. Les paramètres d'authentification doivent être établis, entre autres, en fonction des activités de l'entité et des risques d'accès non autorisés.

La direction des technologies de l'information a la responsabilité de respecter les bonnes pratiques et les principaux standards en vigueur. Pour les paramètres d'authentification, elle doit respecter des standards minimums, qui sont en constante évolution. La figure 13 présente des exemples de bonnes pratiques d'usage des mots de passe auxquelles l'auditeur peut se référer.

FIGURE 13 Exemples de bonnes pratiques d'usage des mots de passe de référence lors de l'audit



Le degré d'usage des bonnes pratiques en vigueur atteste du caractère approprié de la configuration des paramètres de sécurité des mots de passe, considérant également les autres mesures, comme l'authentification multifacteur.

Processus d'attribution, de modification et de révocation des droits d'accès

La figure 14 présente les CGI des processus d'accès notamment aux réseaux, aux applications, aux bases de données ou aux générateurs de rapports pouvant être audités.

FIGURE 14 CGI des processus d'attribution, de modification et de révocation des droits d'accès pouvant être audités

Attribution des droits d'accès	▪ Autorisation du gestionnaire en autorité avant l'attribution des droits d'accès lors de l'arrivée d'un nouvel employé ou d'un contractuel ▪ Utilisation d'une matrice de droits d'accès de référence ▪ Correspondance entre les droits d'accès autorisés et ceux réellement attribués
Révocation des droits d'accès	▪ Révocation (ex. : désactivation ou suppression) des droits d'accès en temps opportun lors du départ ou de l'absence prolongée d'un employé ou d'un contractuel
Modification des droits d'accès	▪ Révocation des droits d'accès en temps opportun lors d'un mouvement de personnel à l'interne (promotion, rétrogradation et mutation) ▪ Autorisation des nouveaux droits d'accès
Séparation des tâches incompatibles	▪ Séparation adéquate des tâches incompatibles entre la personne qui autorise et révise les droits d'accès et celle qui les attribue, les modifie et les révoque
Comptes et droits d'accès génériques ou partagés	▪ Aucun compte utilisateur anonyme ou utilisé par un groupe de personnes afin de favoriser l'imputabilité des actions des utilisateurs
Révision des droits d'accès (surveillance)	▪ Révision périodique de la pertinence des droits d'accès, incluant la révision de la séparation des tâches incompatibles, réalisée par les responsables des différentes directions

Certaines personnes comme les administrateurs de réseaux et de bases de données se voient attribuer des droits d'accès à hauts privilèges qui leur procurent des pouvoirs plus étendus que les utilisateurs réguliers. Outre les CGI présentés dans la figure 14, l'auditeur doit s'assurer que :

- le nombre de personnes bénéficiant de droits d'accès à hauts privilèges est restreint;
- ces droits d'accès et leur utilisation font l'objet d'un suivi périodique et documenté (journalisation des accès et alerte) par une personne indépendante;
- l'utilisation de ces droits d'accès s'effectue avec des codes différents de ceux des droits d'accès réguliers.

En ce qui concerne les CGI des droits d'accès des ressources externes, ils sont audités seulement s'il subsiste un risque significatif qu'une personne non autorisée de l'externe ait accès aux applications financières ou de commerce électronique importantes. Dans ce cas, l'auditeur s'assure que des mécanismes de contrôle adéquats permettent de sécuriser les accès aux systèmes, tels que l'utilisation d'une authentification multifacteur ou d'un réseau privé virtuel (RPV).

CGI des accès physiques

L'audit des CGI des droits d'accès physiques consiste à s'assurer que l'entité a mis en place des mécanismes de sécurité et des contrôles d'accès physiques aux salles informatiques pour assurer une protection adéquate des systèmes informatiques. L'entité doit au minimum s'assurer que :

- les accès physiques sont limités au personnel autorisé, habituellement un groupe restreint du personnel de la direction des technologies de l'information (ex. : portes verrouillées, caméras de surveillance, systèmes d'alarme, registre d'accès, suivi et révision périodique de la liste des détenteurs des droits d'accès).

Selon le risque lié à l'audit des états financiers, l'auditeur effectue une évaluation minimale de la conception et de la mise en place de tels contrôles.

4.3.3 Audit des CGI de la gestion des changements aux systèmes d'information et aux données

L'audit des CGI de la gestion des changements aux systèmes d'information et aux données comprend les contrôles liés :

- au développement et à l'acquisition de nouveaux systèmes;
- à la maintenance des systèmes existants, ainsi qu'à celle des bases de données et de l'infrastructure technologique qui les supportent.

Toute déficience significative en ce qui a trait aux CGI des processus de développement et de maintenance des systèmes d'information augmente le risque d'instabilité des environnements informatiques et par conséquent le risque que des modifications non autorisées soient apportées aux programmes ou aux données financières, ou que des modifications nécessaires ne soient pas effectuées ou soient effectuées inadéquatement, par erreur ou de façon volontaire.

Dans le cadre de l'audit des états financiers, les changements apportés aux systèmes d'information utilisés pour les opérations financières représentent un risque important pour **l'intégrité** des données et de leur traitement. Dans ce contexte, l'audit des CGI vise donc à s'assurer que l'entité a mis en place les contrôles adéquats, comprenant au minimum les contrôles présentés dans la figure 15, qui respectent les bonnes pratiques dans ce domaine.

FIGURE 15 Exemples de bonnes pratiques des CGI des processus de gestion des changements aux systèmes d'information

Intégrité des changements	▪ Des contrôles d'intégrité assurent que l'ensemble des changements est documenté (ex. : surveillance de la journalisation).
Environnements distincts	▪ Les changements apportés aux programmes informatiques par les développeurs sont effectués dans un environnement de développement distinct des environnements de tests et de production. Les développeurs n'ont pas accès à l'environnement de production.
Réalisation de tests	▪ Les tests servant à s'assurer que les programmes informatiques modifiés donnent les résultats attendus sont généralement réalisés par une équipe représentant les utilisateurs. ▪ Les tests sont effectués dans un environnement de tests distinct de celui de production, et ce, pour être certain de ne pas altérer les données financières.
Autorisation par le personnel en autorité	▪ Une autorisation de migrer en production les programmes informatiques est obtenue en temps opportun, notamment du responsable des utilisateurs.
Documentation des systèmes	▪ La documentation des systèmes est mise à jour dans le but de faciliter leur entretien en temps voulu dans le futur.
Séparation des tâches incompatibles	▪ La migration des programmes informatiques de mise en production de l'environnement de tests vers l'environnement de production est effectuée par du personnel différent de celui qui fait la programmation et de celui qui réalise les tests pour respecter le principe de séparation des tâches incompatibles.

Lorsqu'il est difficile d'assurer une séparation adéquate des tâches incompatibles, des contrôles de remplacement compensatoires peuvent être mis en place, tels des activités de supervision des mises en production par la direction des technologies de l'information, notamment la surveillance de la journalisation des mises en production.

Les CGI présentés dans figure 15 doivent aussi être mis en place lors de l'implantation d'un nouveau système informatique, car l'implantation d'un nouveau système implique généralement une conversion de données qui représente un risque important quant à **l'intégrité** des données.

Modification directe aux données

Toute modification aux données financières effectuée en environnement de production (ex. : ajout, modification et suppression de données) sans passer par une application peut représenter un risque majeur en ce qui concerne l'intégrité des données. Ainsi, l'auditeur s'assure que des contrôles des modifications sont en place, soit que les modifications sont :

- autorisées par le propriétaire des données;
- journalisées afin de garantir l'intégrité des modifications et de permettre la vérification a posteriori;
- réalisées en respectant la séparation des tâches incompatibles entre le propriétaire des données qui autorise les modifications et la personne qui modifie les données directement dans les fichiers.

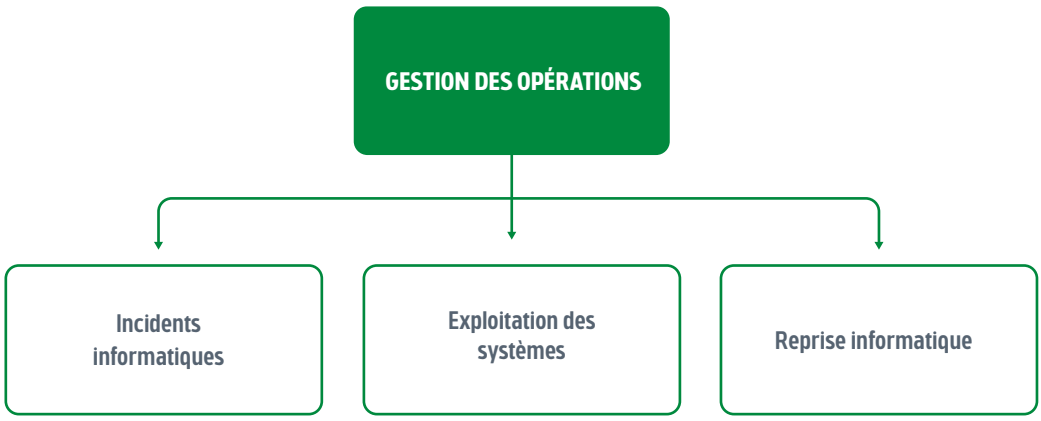
4.3.4 Audit des CGI de la gestion des opérations

La gestion des opérations permet d'assurer la **disponibilité** et l'intégrité de l'information. Selon l'évaluation des risques du recours à l'informatique effectuée, toute déficience significative des CGI de la gestion des opérations a moins d'incidence sur la stratégie d'audit des états financiers que les déficiences des CGI de la gestion des accès et de la gestion des changements aux systèmes d'information et aux données.

Une lacune de contrôle ayant un impact sur la continuité des services informatiques n'empêche généralement pas l'utilisation de la stratégie d'audit des états financiers axée sur les contrôles.

Les derniers CGI pouvant être audités sont donc ceux de la gestion des opérations, qui regroupent les trois types d'opération illustrées dans la figure 16.

FIGURE 16 Opérations ayant un impact sur la continuité des services informatiques dont les CGI peuvent être auditées



CGI de la gestion des incidents informatiques

Les CGI liés à la gestion des incidents informatiques, particulièrement ceux qui peuvent affecter la sécurité de l'information financière, s'avèrent cruciaux pour une entité compte tenu du risque important sur le plan de **l'intégrité** des données. Pour s'assurer d'une saine gestion des incidents informatiques, l'auditeur s'intéresse notamment aux contrôles suivants :

- la mise en place de mécanismes d'enregistrement et d'investigation permettant une détection rapide et une résolution adéquate des incidents, selon leur importance, afin de s'assurer de l'intégralité des données et de la reprise des activités en temps opportun;
- une reddition de comptes à la haute direction aux fins de surveillance par cette dernière des incidents jugés les plus importants.

Cybersécurité

Dans le cadre de la planification du mandat d'audit, l'auditeur doit acquérir une compréhension des processus de l'entité liés à la cybersécurité lui permettant de comprendre et de déterminer les risques. L'évaluation des cyberrisques de même que l'application de certaines procédures d'audit connexes sur les mesures de cybersécurité ne constituent pas une assurance à l'égard de la protection contre les cyberattaques. Par conséquent, aucune opinion n'est exprimée sur le sujet dans le cadre de l'audit.

L'auditeur n'effectue :

- aucun test d'intrusion, mais il s'assure que l'entité effectue la surveillance de la vulnérabilité de son environnement informatique et exécute des tests d'intrusion selon une fréquence et une couverture adéquate;
- aucune investigation détaillée pour s'assurer que les systèmes de prévention et de détection d'intrusions, les pare-feux ou les logiciels antivirus mis en place et maintenus à jour par l'entité auditée (mais il demande si ce type de mesures a été utilisé au cours de l'exercice financier audité et s'il y a lieu d'autres travaux sont exécutés pour évaluer le risque d'atteinte à l'intégrité des données financières).

CGI de la gestion de l'exploitation des systèmes

L'exploitation des systèmes informatiques, en particulier pour les traitements par lots, affecte directement les opérations, et une défaillance à cet égard peut menacer une partie ou l'ensemble des opérations de l'entité. Pour s'assurer du bon déroulement des opérations informatiques, l'auditeur informatique s'assure :

- que l'accès à un planificateur de tâches informatisé servant à établir la séquence des tâches en différé (traitements par lots) est réservé au personnel autorisé;
- qu'une autorisation est exigée pour apporter des changements aux calendriers de production;
- que le suivi des travaux (rapports de rejets ou de fin anormale, etc.) est efficace.

CGI de la gestion de la reprise informatique

La reprise informatique permet à l'entité d'assurer la **disponibilité** de ses systèmes d'information à la suite d'un incident majeur afin de minimiser toute interruption des services essentiels en cas de panne ou d'attaque.

Afin de s'assurer de la capacité de l'entité de poursuivre ses activités en temps opportun lors d'un incident majeur, l'auditeur s'assure :

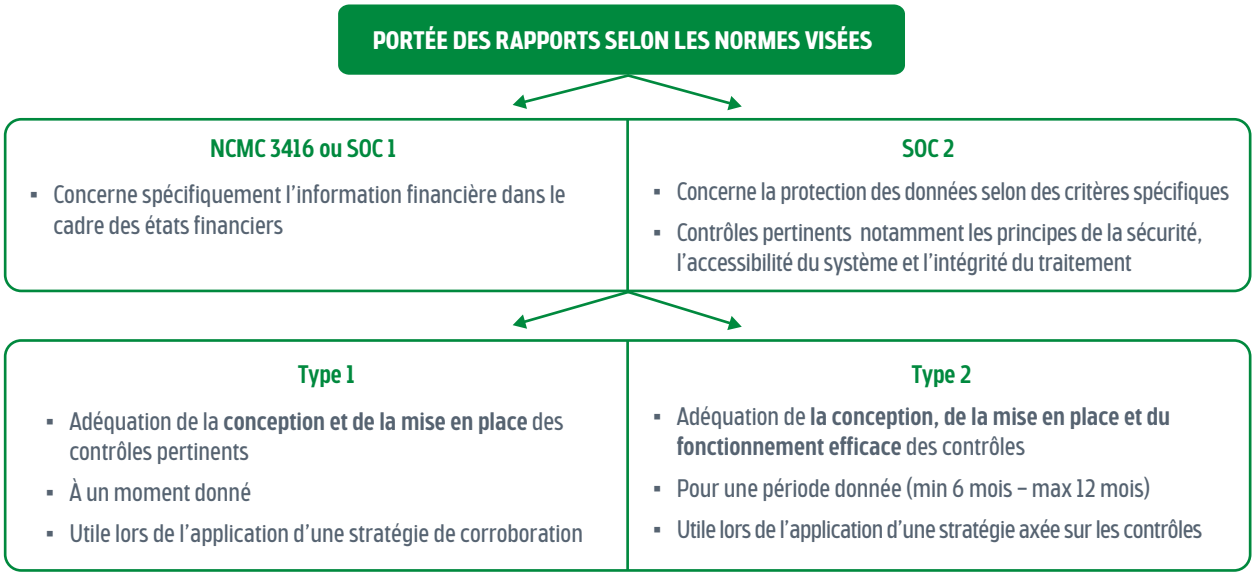
- que la sauvegarde des données et des programmes informatiques est effectuée selon une fréquence appropriée, que les copies des données et des programmes sont conservées ailleurs que dans le centre informatique et que leur intégrité est assurée périodiquement;
- qu'un plan de reprise couvrant les applications importantes existe et qu'il est testé périodiquement, et ce, de façon planifiée.

4.3.5 Autres travaux d'audit

Rapports sur les contrôles de l'impartiteur[6] informatique

La responsabilité de l'entité s'étend aux services impartis (ex. : infonuagique), notamment en ce qui concerne la protection de ses actifs (ex. : gestion des accès) et la préparation de ses états financiers. Une des façons d'exercer sa responsabilité est d'obtenir un rapport d'audit indépendant sur les contrôles de l'impartiteur. Les différents rapports utilisés qui répondent aux normes sont présentés dans la figure 17.

FIGURE 17 Rapports d'audit indépendant sur les contrôles de l'impartiteur



1. Les rapports SOC 3 ne sont normalement pas ou peu utiles dans la cadre de l'audit des états financiers.

6. Dans la norme canadienne d'audit 3416, le terme utilisé pour « impartiteur » est « société de services »

L'auditeur informatique analyse les différents rapports d'audit indépendant obtenus par l'entité. Le rapport le plus utile dans le cadre de l'audit des états financiers est le rapport sur les contrôles d'une société de services, qui répond à la norme canadienne de missions de certification 3416 (NCMC 3416) ou celui qui répond à la norme américaine *System and Organization Controls* (SOC 1).

L'auditeur prend en compte la portée des services impartis pour les systèmes audités. Pour ce faire, il doit notamment :

- acquérir une compréhension des services impartis considérant les trois modèles types, soit :
  - infrastructure en tant que service,
  - plateforme en tant que service,
  - logiciel en tant que service;
- s'assurer que les applications couvertes par le rapport sont pertinentes et en lien avec l'audit des états financiers;
- déterminer les contrôles pertinents et évaluer si leur conception et leur mise en place (réf. : type 1) ou leur efficacité (réf. : type 2) sont adéquates;
- assurer la concordance entre la période couverte par le rapport et celle couverte par l'audit des états financiers (ex. : couverture d'un minimum de 9 mois sur 12 avec une lettre de confort pour les trois derniers mois de l'exercice).

De plus, selon la nature des services impartis et la pertinence des contrôles compte tenu des processus et des risques relatifs d'impact sur les états financiers, l'auditeur peut aussi utiliser un rapport répondant à la norme SOC 2.

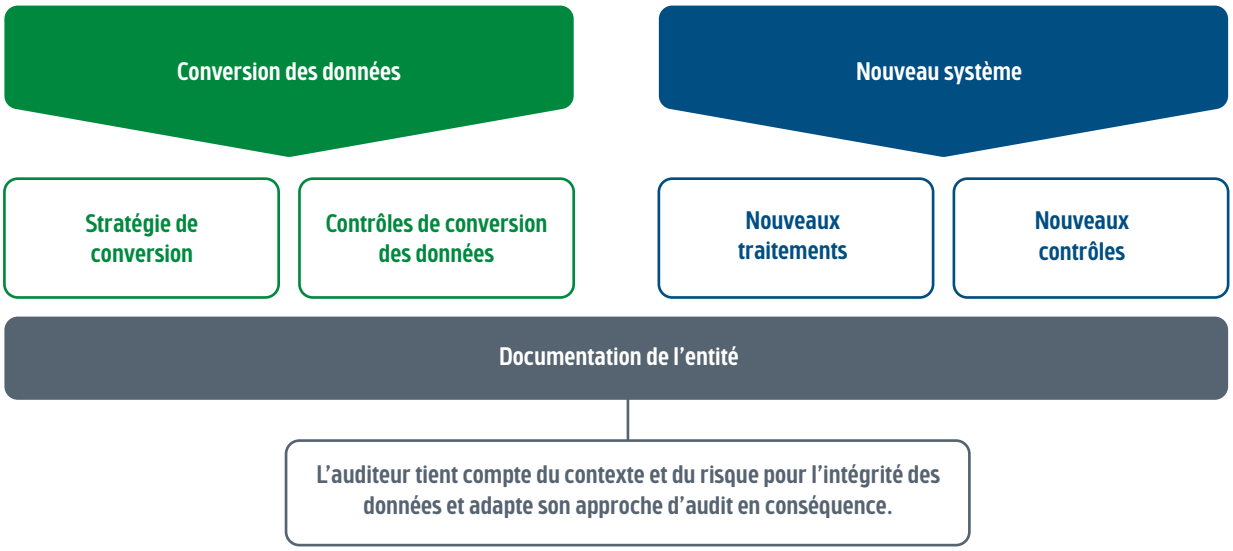
L'auditeur se réfère à la norme canadienne d'audit intitulée *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services* (NCA 402) pour analyser ces rapports d'audit sur les contrôles de l'impartiteur.

Conversion de données

Il est incontournable qu'un jour ou l'autre, l'entité effectue une conversion de données lors de l'implantation d'un nouveau système pertinent pour la préparation des états financiers ou d'une mise à jour importante d'un tel système.

L'entité a la responsabilité d'informer l'auditeur à l'avance de tout changement à cet égard ayant eu cours durant l'exercice financier audité. Elle doit s'assurer a priori de l'intégrité (exhaustivité, exactitude, validité) de la conversion des données et des nouveaux traitements. Enfin, elle doit conserver toute la documentation probante nécessaire aux fins de l'audit. En tenant compte du contexte et du risque d'atteinte à l'intégrité des données, l'auditeur financier, en collaboration avec l'auditeur informatique, adapte sa stratégie d'audit en portant attention aux éléments présentés dans la figure 18.

FIGURE 18 Éléments pouvant être audités lors d'une conversion des systèmes comptables en cours d'année



Jeux d'essai

Selon la stratégie d'audit utilisée, des jeux d'essai sont planifiés et exécutés par l'auditeur financier. Ils sont habituellement effectués une fois par année selon le calendrier convenu avec l'entité. Ils servent à tester les traitements et les contrôles clés au sein des applications ciblées par l'audit (ex. : le grand livre, le système des revenus).

Au besoin, l'auditeur informatique s'assure que l'environnement de tests est équivalent à l'environnement de production. Il peut arriver que l'entité permette à l'auditeur d'effectuer des tests directement dans l'environnement de production. Cette situation a l'avantage d'offrir l'assurance que les traitements sont actuels, contrairement à l'environnement de tests qui peut ne pas être à jour.

Cependant, l'utilisation de l'environnement de production n'est pas sans risque, car il pourrait être altéré lors des tests ou devenir indisponible pour les utilisateurs.

Analyse de données

L'analyse de données regroupe des procédures d'audit servant à dégager et à analyser des tendances, à identifier les anomalies et à obtenir, à partir de populations de données pertinentes, d'autres informations utiles pour l'audit. Lors des travaux d'audit des CGI, l'auditeur utilise entre autres des techniques d'audit assistées par ordinateur (TAAO) perfomantes pour effectuer des analyses. Il est en mesure de mettre en œuvre des procédures pouvant, dans certains cas, porter sur la totalité des éléments de grandes populations de données.

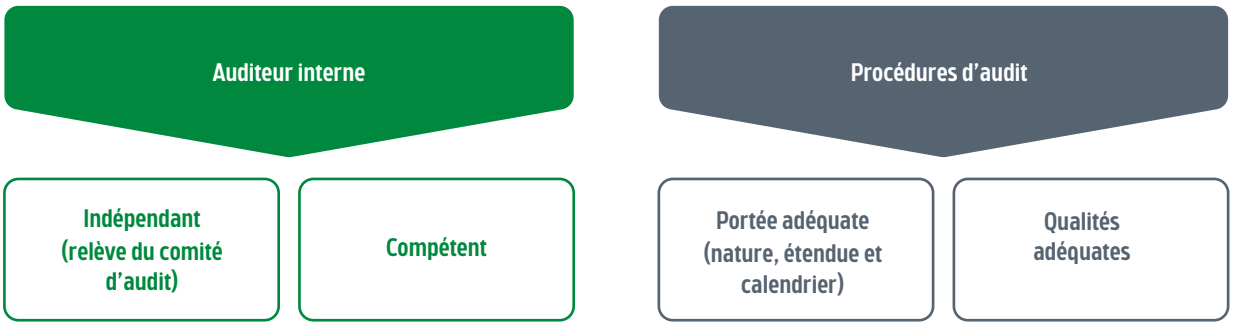
Utilisation des travaux de l'auditeur interne

Dans certaines conditions, l'auditeur informatique peut utiliser les travaux de l'auditeur interne afin notamment de s'assurer :

- de l'intégrité de la conversion des données;
- de la conception et de la mise en place des CGI, ainsi que de leur fonctionnement.

Pour s'appuyer sur des travaux d'audit interne, il s'assure entre autres du respect des éléments présentés dans la figure 19.

FIGURE 19 Éléments considérés avant d'utiliser les travaux de l'auditeur interne



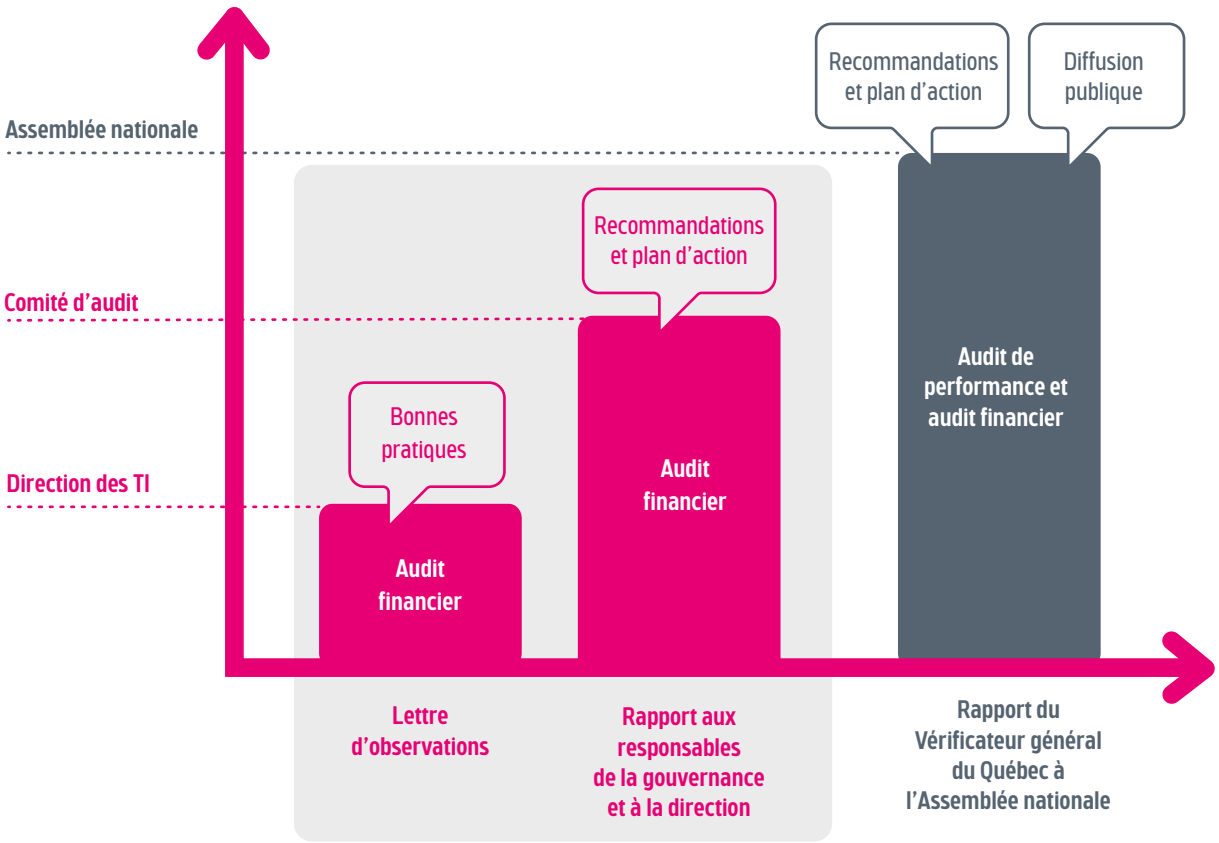
5. COMMUNICATION DES RÉSULTATS ET SUITES DE L'AUDIT

Lors d'un audit des CGI dans le cadre de l'audit des états financiers, l'auditeur informatique rend compte des résultats de son audit dans une lettre d'observations adressée à la direction des technologies de l'information ou dans un rapport aux responsables de la gouvernance et à la direction.

Principales communications du Vérificateur général concernant ses audits

La figure 20 présente, à titre d'information, les principales communications du Vérificateur général découlant de ses travaux d'audit informatique, financier et de performance, ainsi que les destinataires de ces publications.

FIGURE 20 Les différentes communications du Vérificateur général découlant de ses travaux d'audit liés aux technologies de l'information



Lettre d'observations	La lettre d'observations est transmise lorsque les déficiences constatées ne requièrent pas l'intervention des responsables de la gouvernance.
Rapport aux responsables de la gouvernance et à la direction	Le rapport aux responsables de la gouvernance et à la direction est transmis lorsque les déficiences observées pourraient porter atteinte à l'intégrité des données ou de leur traitement et modifier la stratégie d'audit des états financiers. Le rapport est adressé aux membres du comité d'audit de l'entité ou son équivalent ainsi qu'à la direction. Le comité d'audit est informé des recommandations prévues dans un document intitulé *Résultats de l'audit des états financiers*. Contrairement à la lettre d'observations, dans le rapport aux responsables de la gouvernance et à la direction, le Vérificateur général demande : ▪ l'adhésion de la haute direction aux recommandations du Vérificateur général; ▪ les commentaires officiels de la haute direction à l'égard du rapport du Vérificateur général; ▪ un plan d'action qui comprend un responsable et un calendrier de réalisation, qui sera suivi annuellement jusqu'à ce que les déficiences soient corrigées.
Rapport d'audit déposé à l'Assemblée nationale	Il s'agit principalement de rapports d'audit de performance portant sur les technologies de l'information. Plus de détails sur ce type de rapport sont présentés en annexe du présent guide.

Suivi du plan d'action de l'entité dans le cadre de l'audit des états financiers

Le Vérificateur général effectue un suivi annuel de l'application des recommandations formulées dans son rapport en fonction du calendrier de réalisation du plan d'action de l'entité.

L'entité doit lui fournir l'état d'avancement de son plan d'action, comprenant son évaluation de la mise en œuvre des actions prévues et de l'application des recommandations. Le Vérificateur général analyse l'état d'avancement et les éléments probants à l'appui, et formule son appréciation du degré d'application des recommandations jusqu'à ce qu'elles soient appliquées.

Différences entre l'audit des CGI dans le cadre de l'audit des états financiers et l'audit de performance lié aux technologies de l'information

Le Vérificateur général effectue deux types d'audit informatique auprès des entités de son champ de compétence. Outre l'audit des CGI dans le cadre de l'audit des états financiers, dont il est question dans le présent guide, il effectue des audits de performance portant sur l'usage des technologies de l'information. Les principales différences entre ces deux types d'audit sont présentées ci-après.

	AUDIT DES CGI DANS LE CADRE DE L'AUDIT DES ÉTATS FINANCIERS[1]	AUDIT DE PERFORMANCE LIÉ AUX TECHNOLOGIES DE L'INFORMATION
Objectifs	▪ Contribuer à l'opinion de l'auditeur financier sur la fiabilité des états financiers. ▪ Auditer, en fonction des risques, les contrôles informatiques visant l'intégrité des données et des traitements des systèmes nécessaires à la préparation des états financiers.	▪ Auditer les moyens que l'entité met en place pour s'assurer que les ressources à sa disposition sont utilisées de manière économique, efficiente et efficace, et ce, conformément aux lois, aux règlements, aux politiques et aux directives applicables. Les trois principes fondamentaux de sécurité de l'information, soit la disponibilité, l'intégrité et la confidentialité, peuvent faire l'objet d'un audit de performance (figure 3).
Intervention	**Principales normes appliquées** ▪ Normes canadiennes d'audit (NCA)	**Principales normes appliquées** ▪ Normes canadiennes de missions de certification (NCMC) du *Manuel de CPA Canada – Certification*, notamment avec la norme sur les missions d'appréciation directe (NCMC 3001)
	Portée des travaux ▪ Audit des CGI en raison de leur impact sur la préparation des états financiers	**Portée des travaux** ▪ Audit de pratiques de gestion, de contrôle internes, de processus, de programmes, de systèmes d'information
	Caractéristiques ▪ Audit annuel ▪ Vise toutes les entités du champ de compétence du Vérificateur général qui ont la responsabilité de présenter des états financiers (un audit annuel par entité)	**Caractéristiques** ▪ Audit non récurrent annuellement, sauf exception ▪ Vise une ou plusieurs entités, selon le sujet de l'audit
	Suites de l'audit ▪ Rapport sur les déficiences des CGI à l'intention des responsables de la gouvernance et à la direction et réalisation d'un suivi (voir la section 5)	**Suites de l'audit** ▪ Rapport à l'Assemblée nationale et suivi du plan d'action de l'entité ▪ Pour plus d'information sur l'audit de performance, consulter le *Guide à l'intention des entités auditées* sur le site Web du Vérificateur général.

1. Certaines entités ne préparent pas d'états financiers, mais leurs données financières peuvent être auditées par le Vérificateur général dans le cadre de son audit des états financiers consolidés du gouvernement. C'est dans ce contexte que le Vérificateur général pourrait effectuer des travaux d'audit de leurs CGI.

Voici, à titre d'exemples, des rapports d'audit de performance et des études en lien avec les technologies de l'information publiés par le Vérificateur général ces dernières années qui peuvent être consultés sur son site Web :

- Protection des renseignements personnels numériques des usagers du réseau de la santé et des services sociaux (audit de performance, novembre 2023);
- Cybersécurité (étude, novembre 2021);
- Gestion des identités et des accès informatiques (audit de performance, juin 2020);
- Reprise informatique (audit de performance, mai 2018);
- Portrait de la gouvernance et de la gestion des technologies de l'information au gouvernement du Québec (étude, mars 2017).