CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Foire aux questions

La norme NCA 315 et les responsabilités de l'auditeur à l'égard des contrôles généraux informatiques

NOVEMBRE 2023

Avis de non-responsabilité

Le bulletin *ASA 315 and the Auditor's Responsibilities for General IT Controls*, publié en juin 2022 par l'Australian Auditing and Assurance Standards Board (AUASB), a fourni des assises à l'élaboration de la présente FAQ. Il a été utilisé avec la permission de l'AUASB.

La présente foire aux questions vise à aider les professionnels en exercice à mettre en œuvre la norme NCA 315, *Identification et évaluation des risques d'anomalies significatives*, et non à se substituer à la lecture de celle-ci. Seules certaines exigences de la norme y sont abordées.

Synthèse

Les technologies évoluent à un tel rythme et ont une telle incidence sur les organisations qu'il devient difficile de bien comprendre ce qu'on entend par contrôles généraux informatiques, son acronyme CGI et leurs variantes (par exemple, contrôles informatiques généraux). Ces expressions remontent à l'époque où les systèmes informatiques des entreprises étaient constitués d'ordinateurs centraux hébergés dans des centres de données centralisés et gérés par des services de TI. Gardiens des systèmes et applications, ils leur appliquaient uniformément des processus de gestion et contrôles connexes (gestion de la sécurité, modification des programmes, traitement des données) de leur cru. Ainsi est né le terme « contrôles généraux informatiques ».

Toutefois, de tels environnements où la gestion et le contrôle des systèmes et applications informatiques sont centralisés ne sont plus la norme de nos jours. Bien que bon nombre des systèmes et applications d'entreprise soient encore gérés par les services de TI, il est courant que leur gestion soit confiée à différents services ou aux utilisateurs finaux eux-mêmes, voire à des tiers fournisseurs de services.

23-3154

Les contrôles liés au traitement de l'information, y compris ceux concernant la gestion de la sécurité et la modification des programmes, ne se limitent donc pas nécessairement aux systèmes et applications que seul le service des TI gère. Il peut également être question des systèmes, processus et applications qui sont gérés et utilisés par différents services, par les utilisateurs finaux ou par des tiers fournisseurs de services.

La compréhension de l'environnement informatique et l'identification des CGI font partie des exigences auxquelles l'auditeur doit se conformer selon la norme NCA 315. Le présent document ne constitue pas une liste exhaustive des questions que l'auditeur pourrait être amené à se poser; toutefois, il fait ressortir des éléments à prendre en considération pour acquérir une compréhension de l'environnement informatique et de façon plus précise des CGI afin de déterminer si, quand et comment les tester. Voici des exemples de tels éléments :

- L'identification des systèmes et applications susceptibles d'être dotés de contrôles automatisés et des informations destinées à être utilisées comme éléments probants, dont les rapports générés par le système et les données du client reçues sous forme électronique;
- Le cheminement des informations dans les systèmes d'information de l'entité, du déclenchement des opérations à l'enregistrement des informations dans le grand livre général et à leur communication dans les états financiers;
- La façon dont les opérations sont déclenchées au sein de l'entité et dont les informations les concernant sont consignées et mises à jour;
- Les ressources informatiques que l'entité utilise pour les processus liés au déclenchement des opérations, puis à leur documentation, leur mise à jour et leur communication;
- Les différents environnements de traitement dans lesquels les systèmes et applications pertinents pour la préparation des états financiers fonctionnent et sont gérés (par exemple, environnement de traitement informatique central ou décentralisé, systèmes départementaux, ordinateurs des utilisateurs finaux ou tiers fournisseurs de services);
- La responsabilité à l'égard de l'intégrité et de la fiabilité des systèmes, des applications et des informations générées;
- Les processus et contrôles connexes de gestion des risques liés aux TI (modifications non autorisées des données, erreurs de programmation, erreurs de conversion de données, erreurs de saisie de données) dans chaque environnement de traitement;
- La question de savoir si les contrôles pertinents ont été conçus efficacement, ont été mis en place et, s'il y a lieu, ont un fonctionnement efficace.

Questions abordées dans la présente FAQ

Introduction

La présente FAQ vise à aider les auditeurs à comprendre le rôle des CGI dans l'audit des états financiers ainsi que leurs responsabilités à l'égard des CGI.

Il est particulièrement pertinent de s'intéresser à ces points dans la foulée de la révision de la norme NCA 315, *Identification et évaluation des risques d'anomalies significatives*, à l'occasion de laquelle la norme a été mise à jour pour y inclure notamment des éléments relatifs aux technologies à prendre en considération par l'auditeur. Entrée en vigueur pour les audits d'états financiers des périodes ouvertes à compter du 15 décembre 2021, la norme NCA 315 comprend entre autres des annexes nouvelles et d'autres actualisées au sujet de l'acquisition d'une compréhension des TI et des CGI.

L'objectif de la présente publication est de répondre aux questions courantes que se posent les auditeurs au sujet des CGI et de leurs responsabilités en ce qui concerne ceux-ci tout au long de l'audit des états financiers, et non seulement dans le cadre de l'évaluation des risques selon la norme NCA 315. Les réponses à ces questions sont présentées sous forme de FAQ aux pages 8 à 20.

Elles démontrent que l'auditeur n'a pas la responsabilité de comprendre et de tester tous les CGI dans l'environnement de contrôle de l'entité. Sa responsabilité se limite aux contrôles qui sont pertinents pour la préparation des états financiers, comme il est indiqué au paragraphe 26 de la norme NCA 315.

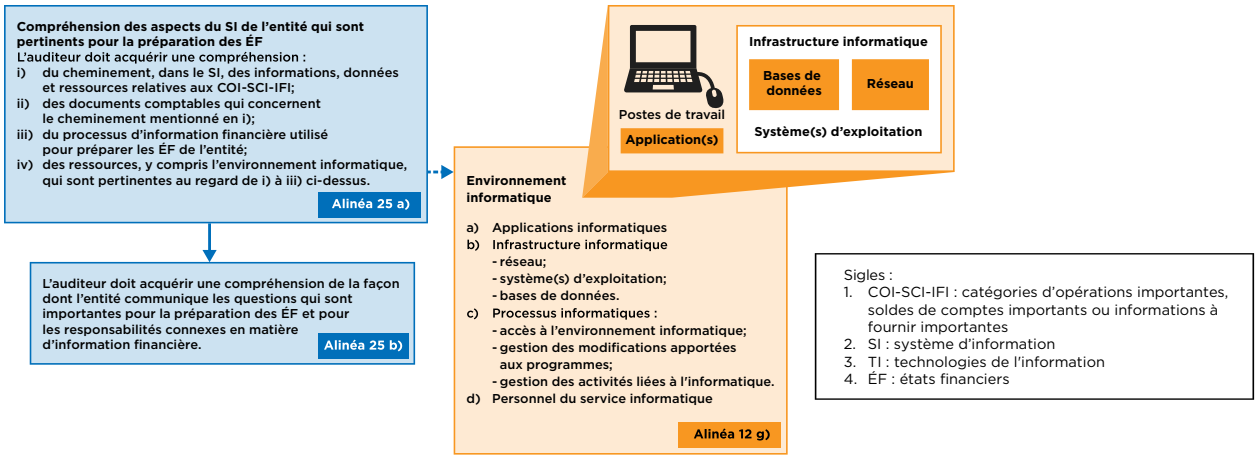
Compréhension de l'environnement informatique et identification des CGI par l'auditeur

La norme NCA 315 comprend de nouvelles modalités importantes en ce qui concerne les technologies et l'audit des états financiers en plus de clarifier les responsabilités de l'auditeur à l'égard des CGI de même que l'incidence de ceux-ci sur l'obtention des éléments probants suffisants et appropriés.

Bien que les CGI ne soient pas à eux seuls suffisamment précis pour répondre aux risques d'anomalies significatives, ils demeurent un élément important du système de contrôle interne de l'entité et favorisent le fonctionnement des contrôles automatisés et l'intégrité des données liées à la préparation des états financiers.

N. B. : Les fragments de diagramme utilisés ci-après sont tirés de l'annexe B, « Compréhension du recours à l'informatique par l'entité », de l'outil d'aide à la mise en œuvre de la NCA 315 révisée.

L'alinéa 25 a) de la norme NCA 315 indique que l'auditeur doit acquérir une compréhension des aspects du système d'information qui sont pertinents pour la préparation des états financiers.



L'acquisition d'une compréhension du système d'information de l'entité est importante, car elle porte entre autres sur les politiques qui définissent le cheminement des opérations et d'autres aspects pertinents pour la préparation des états financiers. Elle aidera l'auditeur à bien identifier les risques d'anomalies significatives au niveau des états financiers et au niveau des assertions. Grâce à la compréhension de l'environnement informatique acquise en application du paragraphe 25 et à l'identification des contrôles en application du paragraphe 26, il se peut que l'auditeur identifie des risques découlant du recours à l'informatique.

Pour déterminer s'il doit identifier les CGI qui répondent à des risques découlant du recours à l'informatique, l'auditeur doit d'abord avoir déterminé si de tels risques existent et, le cas échéant, les avoir identifiés. Selon la nature et les circonstances de la mission, l'équipe de mission peut se demander s'il est nécessaire de faire appel à un spécialiste en informatique ou à d'autres experts pour l'aider à acquérir une compréhension de ces risques et les identifier. Même si l'auditeur ne prévoit pas de tester l'efficacité du fonctionnement des contrôles identifiés, il doit acquérir une compréhension de l'entité et de son environnement, du référentiel d'information financière applicable et des composantes du système de contrôle interne de l'entité, car cette compréhension

peut avoir une incidence sur la nature, le calendrier et l'étendue des procédures de corroboration qu'il concevra[1].

Les diverses applications, l'infrastructure informatique et les processus de gestion connexes, et le personnel de l'entité qui sont pertinents pour la préparation des états financiers forment ce qu'on appelle l'environnement informatique. Lieu de traitement des données et ressources, il peut être composé de plus d'un emplacement, dans l'entité même et auprès de tiers fournisseurs de services (les « environnements de traitement »). Il est important d'identifier les divers environnements de traitement et de les distinguer les uns des autres (et de déterminer s'ils sont pertinents pour la préparation des états financiers), car si les risques liés aux TI (voir l'analyse ci-après) peuvent être similaires, les contrôles visant à atténuer ces risques pourraient être différents.

Selon l'alinéa 26 a) de la norme NCA 315, l'auditeur doit identifier les contrôles visant à répondre aux risques d'anomalies significatives au niveau des assertions.

> Norme NCA 315, alinéa 26 a) :
>
> identifier les contrôles de la composante «activités de contrôle» visant à répondre aux risques d'anomalies significatives au niveau des assertions, c'est-à-dire :
>
> i) les contrôles visant à répondre aux risques identifiés comme des risques importants,
>
> ii) les contrôles afférents aux écritures de journal, y compris les écritures non courantes servant à constater les opérations ou ajustements non récurrents ou inhabituels,
>
> iii) les contrôles dont l'auditeur prévoit de tester l'efficacité du fonctionnement en vue de déterminer la nature, le calendrier et l'étendue des procédures de corroboration, ce qui doit inclure les contrôles visant à répondre aux risques pour lesquels les procédures de corroboration ne peuvent fournir à elles seules des éléments probants suffisants et appropriés,
>
> iv) les autres contrôles qui, selon le jugement professionnel de l'auditeur, sont appropriés pour permettre à celui-ci d'atteindre les objectifs énoncés au paragraphe 13 en ce qui a trait aux risques au niveau des assertions[.]

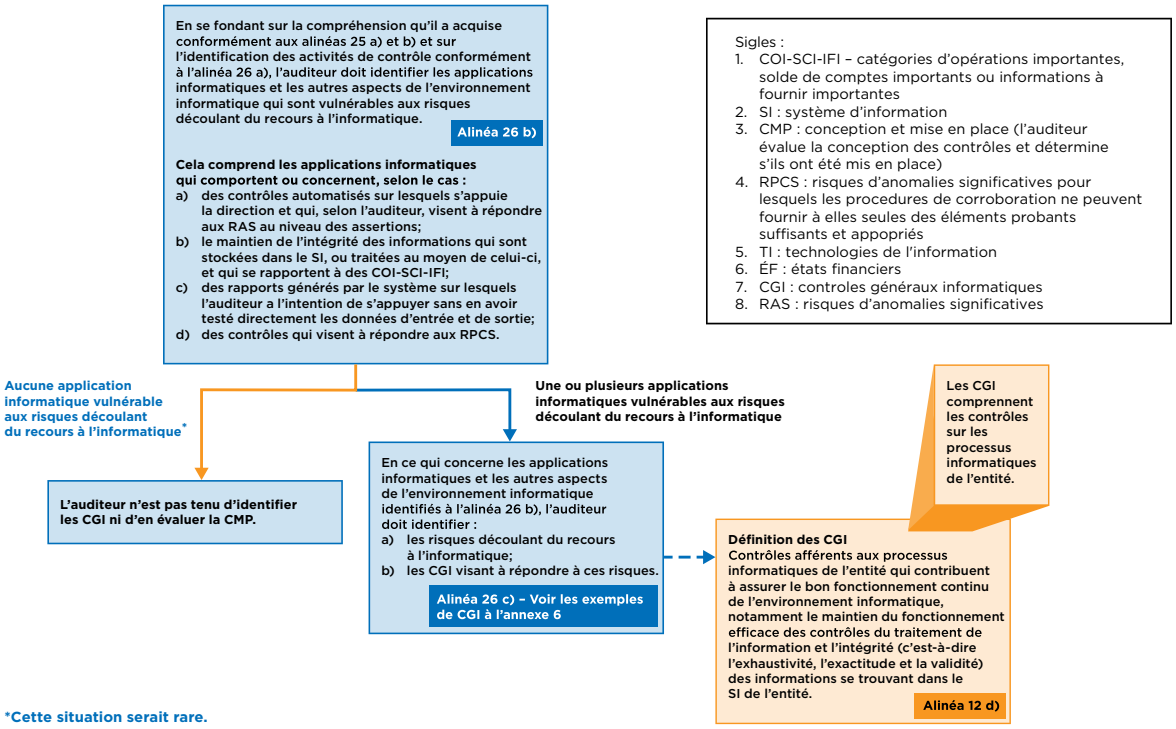
Ces contrôles peuvent être des contrôles du traitement de l'information (voir la question 2).

L'auditeur doit identifier, en fonction de la compréhension acquise en application de l'alinéa 25 a) et des contrôles identifiés selon l'alinéa 26 a), les applications informatiques et les autres aspects de l'environnement informatique qui sont vulnérables aux risques découlant du recours à l'informatique (voir la question 1).

1 Voir les modalités d'application énoncées au paragraphe A125 de la norme NCA 315.

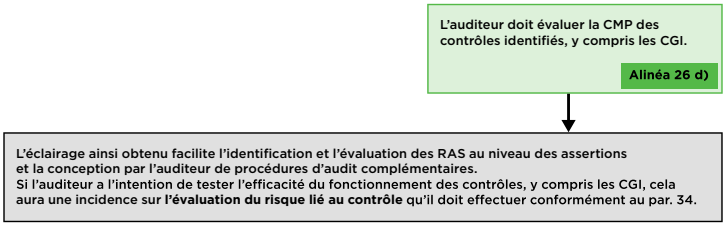
Lorsqu'aucune application ou autre composante de l'environnement informatique n'est vulnérable à des risques découlant du recours à l'informatique, il n'est pas nécessaire d'identifier les CGI ni d'évaluer l'efficacité de leur conception et de déterminer s'ils ont été mis en place.

L'auditeur détermine s'il existe des risques découlant du recours à l'informatique et, le cas échéant, il y répond.



Outre ce dont il prend connaissance dans les rapports générés par le système, l'auditeur peut aussi obtenir, pour les besoins des procédures d'audit, des données directement du client sous forme électronique pour lesquelles il doit également identifier les applications et les autres aspects pertinents du ou des environnements de traitement qui sont vulnérables aux risques découlant du recours à l'informatique.

Une fois qu'il a identifié les contrôles mentionnés aux alinéas 26 a) et c), l'auditeur est tenu de procéder à une évaluation.



Paragraphes 25 et 26 de la norme NCA 315 : en quelques mots

Le paragraphe 25 de la norme NCA 315 jette les fondements de cette norme en mettant l'accent sur l'importance d'acquérir une compréhension du système d'information et des communications de l'entité pour identifier et évaluer les risques d'anomalies significatives. L'acquisition d'une compréhension du système d'information est donc essentielle pour évaluer si ce système contribue adéquatement à la préparation de l'information financière.

Le paragraphe 26 de la norme NCA 315 fournit des précisions sur l'acquisition d'une compréhension du système d'information, notamment en ce qui concerne les CGI. Il précise que l'auditeur doit identifier, pour les contrôles de la composante « activités de contrôle » qu'il a identifiés comme visant à répondre aux risques d'anomalies significatives au niveau des assertions, les applications informatiques et les autres aspects de l'environnement informatique qui pourraient être vulnérables aux risques découlant du recours à l'informatique ainsi que les CGI connexes. Les CGI sont les contrôles généraux qui permettent d'assurer la sécurité et la fiabilité de l'infrastructure informatique sous-tendant les processus d'information financière.

La compréhension qu'il acquiert permet à l'auditeur d'identifier et d'évaluer les risques d'anomalies significatives, les risques liés aux TI et les incidences potentielles sur les états financiers, ce qui lui permet de planifier et de mettre en œuvre des procédures d'audit efficaces conçues en réponse à ces risques en particulier.

Foire aux questions

Question 1 – Quels sont les risques découlant du recours à l'informatique?

Selon l'alinéa 12 i) de la norme NCA 315, l'expression « risques découlant du recours à l'informatique » s'entend de :
la possibilité que la conception ou le fonctionnement des contrôles du traitement de l'information soient inefficaces ou les risques que l'intégrité des informations (c'est-à-dire l'exhaustivité, l'exactitude et la validité des opérations et des autres informations) ne soit pas maintenue au sein du système d'information de l'entité, en raison de l'inefficacité de la conception ou du fonctionnement des contrôles se rapportant aux processus informatiques de l'entité.

Pour les contrôles de la composante « activités de contrôle » qu'il a identifiés en application de l'alinéa 26 a), l'auditeur est tenu d'identifier les applications et les autres aspects du ou des environnements de traitement dans lesquels ces applications fonctionnent qui sont vulnérables aux risques découlant du recours à l'informatique. Les « risques découlant du recours à l'informatique » comprennent notamment les risques associés à un appui inapproprié sur des applications informatiques qui ne traitent pas les données avec exactitude, qui traitent des données inexactes, ou les deux. Voici des exemples de tels risques :

- Accès non autorisé aux données pouvant aboutir à des destructions ou modifications inappropriées de données, y compris l'enregistrement d'opérations non autorisées ou inexistantes ou l'enregistrement incorrect d'opérations. L'accès de multiples utilisateurs à une base de données commune peut poser des risques particuliers;
- Possibilité que des membres du personnel obtiennent des privilèges d'accès supérieurs à ceux qui sont nécessaires pour l'exercice de leurs fonctions, et que la séparation des tâches se trouve ainsi compromise;
- Modifications non autorisées des données dans les fichiers maîtres;
- Modifications non autorisées d'applications ou d'autres aspects d'un environnement de traitement;
- Non-réalisation des modifications nécessaires d'applications ou d'autres aspects d'un environnement de traitement;
- Interventions manuelles inappropriées;
- Perte possible de données ou incapacité d'accéder aux données requises.

L'Annexe 5 de la norme NCA 315 fournit des indications utiles pour l'identification des risques découlant du recours à l'informatique.

Lorsque des applications informatiques sont identifiées par l'auditeur comme étant vulnérables aux risques découlant du recours à l'informatique, il y a généralement certains aspects de l'infrastructure informatique qui sont vulnérables à ces risques. Comme il a été mentionné précédemment, les autres aspects de l'environnement informatique comprennent l'infrastructure informatique, les processus informatiques et le personnel des TI.

Question 2 – Que sont les CGI et en quoi diffèrent-ils des contrôles du traitement de l'information?

Que sont les CGI?

Selon l'alinéa 12 d) de la norme NCA 315, les CGI sont :
les 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 (c'est-à-dire l'exhaustivité, l'exactitude et la validité) des informations se trouvant dans le système d'information de l'entité.

Les CGI forment donc une réponse aux risques découlant du recours à l'informatique. Il peut s'agir de contrôles manuels, de contrôles manuels reposant sur des TI ou de contrôles automatisés. Voici quelques exemples, tirés de l'Annexe 6 de la norme NCA 315, de risques découlant du recours à l'informatique et de CGI pouvant être mis en place pour y répondre.

Exemples de risques découlant du recours à l'informatique	Processus informatique	Exemples de CGI[2]
Privilèges d'accès : Utilisateurs détenant des privilèges d'accès supérieurs à ceux qui sont nécessaires pour l'exercice de leurs fonctions, ce qui peut compromettre la séparation des tâches.	Gestion de l'accès	La nature et l'étendue des privilèges d'accès modifiés ou nouvellement attribués sont approuvées par la direction, notamment en ce qui concerne les rôles/profils standardisés d'utilisateurs des applications, les opérations donnant lieu à des informations financières critiques et la séparation des tâches.
Applications : Modification inappropriée des systèmes/programmes d'application dotés de contrôles automatisés pertinents (paramètres configurables, algorithmes/calculs automatisés, extraction automatisée des données, etc.) ou de fonctionnalités logiques permettant de générer des rapports.	Gestion des changements	Les modifications apportées aux applications sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.
Planification des travaux : Traitement inexact, incomplet ou non autorisé des données dans les systèmes, programmes ou travaux de production.	Gestion des opérations informatiques	Seuls les utilisateurs autorisés peuvent effectuer la mise à jour des travaux par lots (avec ou sans interface) dans le logiciel de planification des travaux.

Les CGI sont généralement des contrôles indirects qui favorisent le fonctionnement de contrôles du traitement de l'information et qui sont mis en œuvre au niveau des applications, des bases de données, des systèmes d'exploitation ou du réseau[3].

Que sont les contrôles du traitement de l'information?

Selon l'alinéa 12 e) de la norme NCA 315, sont des contrôles du traitement de l'information : les contrôles qui concernent le traitement de l'information dans les applications informatiques ou les processus manuels du système d'information de l'entité et qui visent à **répondre directement aux risques liés à l'intégrité des informations** (c'est-à-dire l'exhaustivité, l'exactitude et la validité des opérations et des autres informations).

2 Voir l'Annexe 6 de la norme NCA 315 pour d'autres exemples de risques et de contrôles pouvant être mis en place pour y répondre.

3 Norme NCA 315, paragraphe A96.

Les contrôles du traitement de l'information sont généralement des contrôles directs qui visent à répondre aux risques d'anomalies significatives au niveau des assertions[4]. Ils peuvent dépendre d'autres contrôles (par exemple, de CGI ou d'autres contrôles du traitement de l'information tels que ceux qui gèrent l'accès au code source d'un contrôle du traitement de l'information) pour fonctionner efficacement.

Les contrôles du traitement de l'information comprennent les contrôles liés aux autorisations et aux approbations, aux rapprochements, aux vérifications (comme les contrôles d'édition ou de validation), aux calculs automatisés, à la séparation des tâches ainsi qu'aux contrôles physiques ou logiques, y compris ceux qui assurent la sauvegarde des actifs. L'auditeur se concentre sur ce type de contrôles lorsqu'il identifie des contrôles en application de l'alinéa 26 a)[5].

Il peut s'agir de contrôles automatisés (intégrés aux applications), de contrôles manuels (par exemple, les contrôles sur les données d'entrée ou de sortie) ou de contrôles manuels reposant sur des TI. Voici des exemples courants de ce type de contrôles :

- Contrôle automatisé – contrôle à triple rapprochement intégré au progiciel comptable de l'entité;
- Contrôle manuel reposant sur des TI – examen mensuel par la direction d'un rapport d'anomalies concernant la paie pour déterminer si des modifications inhabituelles ou non autorisées ont été apportées aux informations sur la rémunération. L'examen est effectué manuellement par le directeur, mais il repose sur les contrôles du traitement de l'information sous-tendant le rapport.

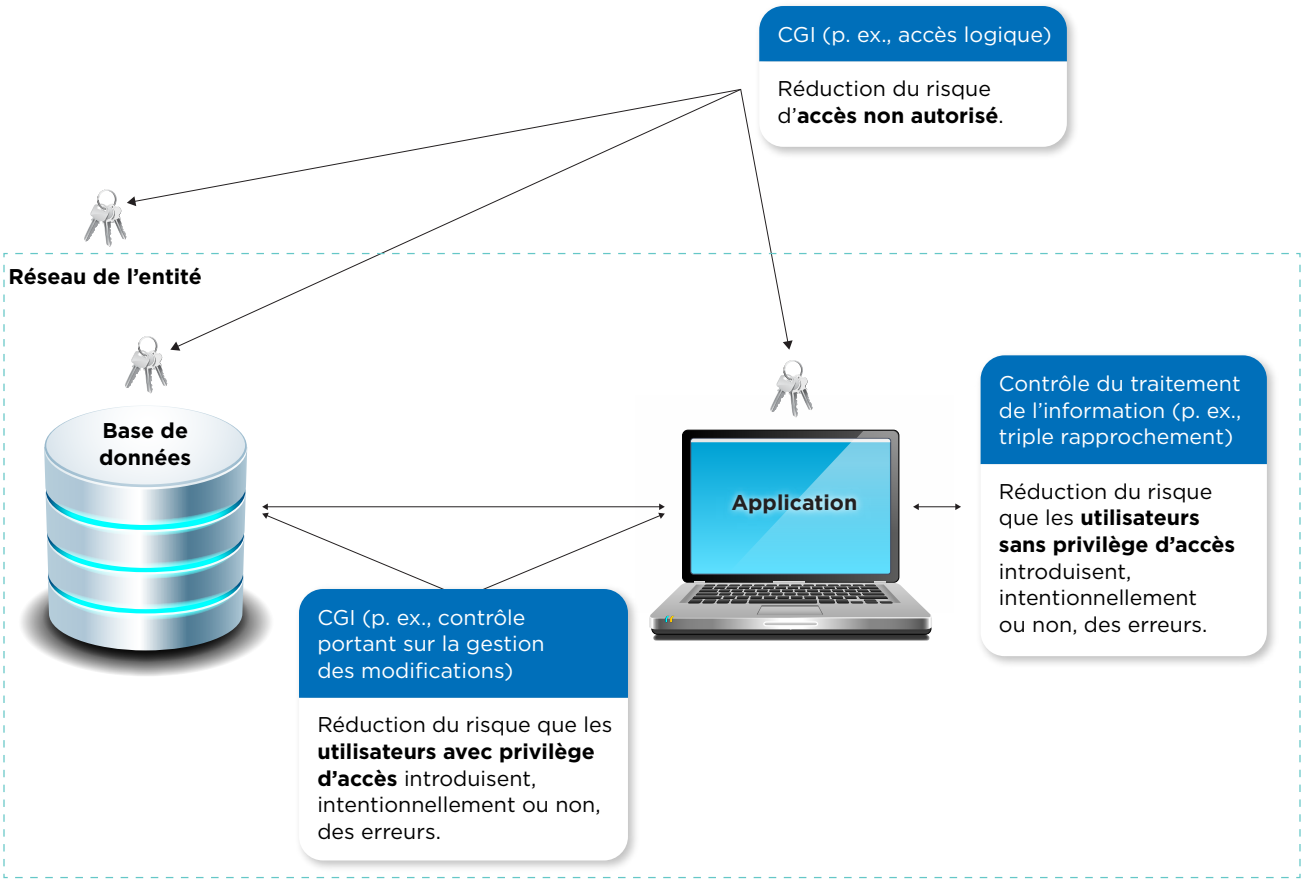
En quoi les contrôles du traitement de l'information diffèrent-ils des CGI?

Les deux types de contrôles diffèrent essentiellement quant au niveau auquel ils agissent et à ce qu'ils visent à prévenir ou à détecter et à corriger. Les contrôles du traitement de l'information sont généralement axés sur la fiabilité et l'intégrité des données au niveau des opérations propres à chaque application, alors que les CGI ont une portée plus large et englobent les contrôles qui permettent d'assurer la sécurité et la fiabilité de l'infrastructure informatique. Ces deux types de contrôles sont essentiels pour assurer l'intégrité, l'accessibilité et la fiabilité des systèmes d'information de l'entité, et ils jouent un rôle dans l'évaluation des risques d'anomalies significatives dans les états financiers.

4 Norme NCA 315, paragraphes A5 et A6.

5 Norme NCA 315, paragraphe A148.

Figure 1 - Contrôles généraux informatiques (CGI) et contrôles du traitement de l'information



Ainsi, un contrôle à triple rapprochement (voir la figure 1) programmé dans une application est un exemple de contrôle du traitement de l'information (en l'occurrence, un contrôle automatisé) conçu pour réduire le risque d'erreurs dans les données financières; il ne cible que les opérations pour lesquelles il existe un bon de commande, un bordereau d'expédition et une facture.

Des CGI peuvent être conçus pour réduire les risques découlant du recours à l'informatique qui sont liés à l'accès inapproprié aux données pouvant aboutir à des destructions ou modifications inappropriées de données, y compris l'enregistrement d'opérations non autorisées ou inexistantes ou l'enregistrement incorrect d'opérations. Ils peuvent aussi être conçus pour réduire les risques découlant du recours à l'informatique qui sont liés à la possibilité que des membres du personnel obtiennent des privilèges d'accès supérieurs à ceux qui sont nécessaires pour l'exercice de leurs fonctions, et que la séparation des tâches se trouve ainsi compromise.

Voici d'autres exemples de CGI :

- Les contrôles intégrés aux processus de gestion des privilèges d'accès logiques à une application, qui visent à empêcher l'accès par des utilisateurs non autorisés et, de ce fait, à réduire le risque d'opérations erronées ou frauduleuses, mais qui n'empêchent généralement pas les utilisateurs autorisés de commettre des erreurs;

- Les contrôles intégrés aux processus de gestion des privilèges d'accès logiques à une base de données, qui visent à réserver à certains utilisateurs la capacité d'apporter des modifications aux données de l'entité (autrement que lors du traitement d'une opération dans l'application) et, de ce fait, à réduire le risque de manipulation erronée ou frauduleuse des données, mais qui n'empêchent généralement pas les utilisateurs autorisés de faire de telles manipulations;
- Les contrôles intégrés aux processus de gestion de la modification d'une base de données ou d'une application, qui visent à réduire le risque que des modifications apportées à l'application ou à la base de données amènent les systèmes à fonctionner d'une façon qui ne correspond pas aux objectifs de la direction.

Une application est l'interface que la plupart des utilisateurs voient (par exemple, SAP et People Soft), c'est-à-dire le système au moyen duquel ils entrent et examinent les données. L'application est en fait stockée dans une base de données sous-jacente à laquelle seuls des utilisateurs privilégiés (généralement le personnel des TI) peuvent accéder. L'auditeur devrait, même lorsqu'il se concentre sur les risques liés aux applications, tenir compte également des risques découlant d'autres éléments de l'environnement informatique, comme les bases de données et les membres du personnel qui ne font pas de saisie de données dans les applications, mais qui ont un accès privilégié aux bases de données.

Il convient de souligner que les processus informatiques, de même que les CGI correspondants intégrés à ces processus, peuvent varier d'un environnement de traitement à l'autre dans l'organisation :

- ils peuvent être centralisés (service des TI de l'entité) et parfois s'appliquer à plusieurs systèmes d'application;
- ils peuvent être décentralisés (service précis responsable de l'application, par exemple le service des finances qui gère l'application du grand livre général) et propres à chaque application;
- ils peuvent être centrés sur les utilisateurs (feuille de calcul conçue et gérée par l'utilisateur final) et propres à chacun d'eux;
- ils peuvent être externalisés (processus de gestion des applications d'un tiers fournisseur de services pour le traitement de la paie de l'entité).

En résumé, les contrôles du traitement de l'information sont en réponse aux risques associés à l'intégrité des informations (c'est-à-dire l'exhaustivité, l'exactitude et la validité des opérations et des autres informations) d'une application donnée, tandis que les CGI ont une portée plus grande et contribuent à assurer la bonne marche de l'environnement informatique, dont le fonctionnement efficace des contrôles du traitement de l'information et l'intégrité des informations se trouvant dans le système d'information de l'entité. Lorsque des contrôles du traitement de l'information sont identifiés comme étant vulnérables aux risques découlant du recours à l'informatique et que des CGI sont identifiés en tant que réponses à ces risques, ces deux types de contrôles ont une incidence sur l'identification et l'évaluation des risques d'anomalies significatives dans les états financiers.

Question 3 – Quand faut-il évaluer la conception d'un CGI et déterminer s'il a été mis en place?

Selon l'alinéa 26 d) de la norme NCA 315[6], l'auditeur est tenu, pour chacun des CGI identifiés comme des réponses aux risques découlant du recours à l'informatique, d'évaluer si la conception du contrôle est efficace pour favoriser le fonctionnement d'autres contrôles et de déterminer si le contrôle a été mis en place. Lorsque des risques découlant du recours à l'informatique et des CGI visant à y répondre sont identifiés, l'auditeur doit évaluer la conception des CGI et déterminer s'ils ont été mis en place, qu'il prévoie ou non de tester l'efficacité de leur fonctionnement en réponse à son évaluation des risques d'anomalies significatives.

L'évaluation de la conception d'un contrôle identifié implique pour l'auditeur de considérer si le contrôle, seul ou en association avec d'autres, a la capacité de prévenir, ou de détecter et corriger, les anomalies significatives. Pour déterminer si un contrôle a été mis en place, il faut s'assurer qu'il existe et que l'entité l'utilise, ce qui ne peut pas être effectué uniquement au moyen de demandes d'informations. Des procédures supplémentaires, comme l'observation de l'application du contrôle ou l'inspection de documents et de rapports, peuvent corroborer la demande d'informations au sujet de la manière dont le contrôle a été conçu ou mis en place, ou peuvent fournir à l'auditeur de nouvelles informations susceptibles d'avoir une incidence sur son évaluation des risques et ses réponses à celle-ci.

L'auditeur pourrait devoir faire appel à des personnes possédant des compétences spécialisées, comme des auditeurs en TI (ou les auditeurs de sociétés de services; voir la question 9), afin de les aider à :

- comprendre les applications informatiques, l'infrastructure informatique et les processus informatiques;
- identifier les risques découlant du recours à l'informatique;
- identifier les CGI visant à répondre aux risques découlant du recours à l'informatique;
- évaluer la conception des CGI pertinents, déterminer s'ils ont été mis en place et, s'il y a lieu, tester l'efficacité de leur fonctionnement.

Selon la norme NCA 220 (révisée), *Gestion de la qualité d'un audit d'états financiers*, c'est l'associé responsable de la mission qui doit déterminer que les membres de l'équipe de mission, ainsi que les experts externes choisis par l'auditeur et les auditeurs internes fournissant une assistance directe qui ne font pas partie de cette équipe, ont collectivement la compétence et les capacités appropriées, notamment suffisamment de temps, pour réaliser la mission[7].

6 Voir les modalités d'application énoncées aux paragraphes A175 à A181 de la norme NCA 315 pour obtenir des indications supplémentaires.

7 Voir le paragraphe 26 de la norme NCA 220 (révisée).

Question 4 – Quand faut-il tester l'efficacité du fonctionnement des CGI?

Lorsque l'auditeur prévoit de tester, en réponse à son évaluation des risques d'anomalies significatives, l'efficacité du fonctionnement de contrôles du traitement de l'information qu'il a identifiés et que des CGI y sont liés, il détermine s'il est nécessaire, en vue de s'appuyer sur les contrôles identifiés, d'obtenir des éléments probants attestant l'efficacité du fonctionnement des CGI dans l'environnement de traitement.

Autrement, il n'est pas tenu de tester l'efficacité du fonctionnement de CGI connexes.

Si l'auditeur conclut qu'un CGI est déficient, mais qu'il prévoit tout de même de tester l'efficacité du fonctionnement du contrôle identifié, il prend en considération la nature des risques connexes découlant du recours à l'informatique afin de disposer d'une base pour les procédures supplémentaires qui permettront de répondre à son évaluation des risques d'anomalies significatives. Ces procédures supplémentaires peuvent notamment servir à déterminer :

- si les risques connexes découlant du recours à l'informatique se sont matérialisés;
- s'il y a des contrôles de remplacement, des contrôles redondants ou d'autres contrôles qui fonctionnent efficacement et dont le niveau de précision est suffisant pour répondre aux risques connexes découlant du recours à l'informatique.

Bien que l'auditeur teste généralement l'efficacité du fonctionnement de CGI dans le but d'étayer son évaluation de l'efficacité du fonctionnement d'un contrôle du traitement de l'information, les éléments probants qu'il obtient peuvent aussi lui être utiles dans d'autres situations, comme les suivantes :

- Procédures analytiques de corroboration – L'auditeur qui a besoin d'éléments probants sur la fiabilité de données qu'il compte utiliser dans le cadre de ces procédures pourrait vouloir s'appuyer sur les CGI s'il détermine que la meilleure façon d'obtenir ces éléments probants est de tester l'efficacité du fonctionnement des contrôles du traitement de l'information. Les tests d'efficacité du fonctionnement fournissent alors des éléments probants sur l'exhaustivité, l'exactitude et la validité des données (par exemple, les taux unitaires d'une liste maîtresse devant servir à recalculer la valeur d'une certaine catégorie d'opérations);
- Contrôles afférents aux écritures de journal[8] – Lorsque l'auditeur teste des écritures de journal comportant des écritures non courantes, il peut choisir de tester l'efficacité du fonctionnement des CGI se rapportant à la gestion des autorisations relatives à l'enregistrement des écritures de journal non courantes;

8 Voir l'outil d'aide à la mise en œuvre de la NCA 315 révisée élaboré par CPA Canada; les questions N2 et N3 portent sur les écritures de journal.

- Rapports générés par un système ou données du client reçues sous forme électronique – Lorsque les procédures de corroboration s'appuient sur de telles informations, l'auditeur peut tester l'efficacité du fonctionnement des CGI visant à répondre aux risques de modification non autorisée ou inappropriée du rapport ou des données (en plus de tester les contrôles portant sur l'exhaustivité et l'exactitude du rapport ou des données). Voir la question 7 pour plus d'informations à ce sujet;
- Interface automatisée – Lorsqu'il y a transmission d'informations entre deux applications ou systèmes (par exemple, les données relatives aux ventes enregistrées dans le système de point de vente d'un magasin de détail sont automatiquement transmises au système comptable ou de grand livre général qui lui est associé), l'auditeur peut tester l'efficacité du fonctionnement des CGI visant à répondre aux risques de traitement inexact, incomplet ou non autorisé de ces données.

Question 5 – En quoi la complexité de l'environnement informatique de l'entité influe-t-elle sur la nature des CGI?

La nature des CGI visant à répondre aux risques découlant du recours à l'informatique peut varier selon la complexité de l'environnement informatique. L'Annexe 6 de la norme NCA 315 donne des exemples de risques courants découlant du recours à l'informatique et de CGI pouvant être mis en place pour y répondre, selon la complexité des applications informatiques.

> **Exemple :**
> On peut dire que la complexité des CGI est fonction de celle de l'environnement informatique. Ainsi, les CGI de l'entité utilisant des applications commerciales largement répandues dont le code source ne lui est pas accessible et dont les mises à jour fournies par le fournisseur font l'objet d'une revue, d'une évaluation et d'un test avant leur déploiement pourraient être moins complexes que ceux de l'entité où les processus de gestion des privilèges d'accès des utilisateurs et de modification d'applications ou d'autres composantes informatiques sont complexes, font intervenir plusieurs personnes et peuvent faire appel à des outils automatisés ou à des applications de gestion des TI.

L'auditeur exerce son jugement professionnel pour déterminer l'étendue des travaux à mettre en œuvre à l'égard des CGI. Il n'est pas tenu d'identifier tous les contrôles qui font partie de l'environnement de contrôle de l'entité, ni même tous ceux qui font partie de son ou de ses environnements de traitement.

Question 6 – Les CGI doivent-ils être testés chaque année?

Certaines procédures d'audit liées aux CGI doivent être mises en œuvre chaque année, notamment :

- l'acquisition d'une compréhension des processus informatiques;
- l'identification des CGI visant à répondre aux risques découlant du recours à l'informatique (voir la question 1);

- lorsque des risques découlant du recours à l'informatique et des CGI visant à y répondre ont été identifiés, l'évaluation de la conception des CGI et la vérification de leur mise en place (voir la question 3).

En ce qui concerne les tests de l'efficacité du fonctionnement des CGI, les normes d'audit permettent aux auditeurs d'utiliser, dans certaines circonstances, des éléments probants sur l'efficacité du fonctionnement des contrôles recueillis au cours des audits précédents. Le paragraphe 13 de la norme NCA 330, *Réponses de l'auditeur à l'évaluation des risques*, énonce les éléments dont l'auditeur doit tenir compte pour déterminer s'il est approprié d'utiliser des éléments probants sur l'efficacité du fonctionnement des contrôles obtenus lors des audits précédents. Toutefois, les normes ne précisent pas explicitement si cela vaut aussi pour les CGI. Comme les CGI contribuent à assurer le bon fonctionnement continu des contrôles du traitement de l'information, l'auditeur peut décider de les tester annuellement.

Dans certains cas, les éléments probants recueillis au cours des audits précédents peuvent de nouveau servir d'éléments probants lorsque l'auditeur met en œuvre des procédures d'audit confirmant qu'ils sont toujours pertinents et fiables. Par exemple, lors d'un audit précédent, l'auditeur peut avoir déterminé qu'un CGI fonctionnait comme prévu. Il peut alors recueillir des éléments probants qui lui permettent de déterminer si le CGI en question a fait l'objet de modifications affectant l'efficacité continue de son fonctionnement, par exemple par des demandes d'informations auprès de la direction et par l'inspection des journaux des interventions indiquant les contrôles qui ont été modifiés. La prise en considération des éléments probants portant sur ces modifications peut entraîner soit une augmentation, soit une diminution des éléments probants à obtenir pendant la période en cours relativement à l'efficacité du fonctionnement de ce CGI.

Question 7 – Si je prévois de tester l'efficacité du fonctionnement d'un CGI, quel sera l'impact si sa conception et sa mise en œuvre se révèlent inadéquates ou si son fonctionnement est inefficace?

Selon le paragraphe 34 de la norme NCA 315, si l'auditeur prévoit de tester l'efficacité du fonctionnement des CGI, il doit évaluer le risque lié au contrôle dans le cadre de son évaluation des risques d'anomalies significatives au niveau des assertions.

Le fait que l'auditeur prévoie ou non de tester l'efficacité du fonctionnement des CGI dépend de ses attentes quant au fonctionnement efficace de ceux-ci et lui fournit une base pour évaluer le risque lié au contrôle. Les attentes de l'auditeur à cet égard sont fondées sur son évaluation de la conception des contrôles identifiés en application du paragraphe 26 de la norme et sur sa vérification de leur mise en place.

Si les CGI n'ont pas été conçus ou mis en place de façon appropriée, l'auditeur en tient compte lorsqu'il évalue le risque lié au contrôle en application du paragraphe 34 de la norme NCA 315[9]. Lorsqu'un CGI particulier n'a pas été conçu ou mis en place de façon appropriée, l'auditeur peut se demander dans le cadre de son évaluation du risque lié au contrôle :

9 Norme NCA 315, paragraphe A229.

- s'il y a des CGI de remplacement ou d'autres contrôles visant à répondre aux risques connexes découlant du recours à l'informatique;

- s'il est en mesure de concevoir des procédures de corroboration adaptées pour répondre aux risques découlant du recours à l'informatique.

Exemples :

- Lors de son évaluation de la conception des contrôles relatifs à la modification des applications, l'auditeur a conclu que les contrôles visant à assurer que toutes les modifications ont été autorisées par la direction n'ont pas été conçus de façon appropriée. Toutefois, d'autres contrôles de la même nature, dont des contrôles concernant l'exhaustivité et l'exactitude du journal des modifications apportées aux applications, ont été conçus de façon appropriée et fonctionnent efficacement. L'auditeur a déterminé qu'il pouvait examiner manuellement le journal et vérifier si des modifications non autorisées sont survenues au cours de la période, auquel cas l'efficacité du fonctionnement des contrôles du traitement de l'information qui sont automatisés s'en trouverait affectée.
- Après avoir passé en revue les processus de gestion d'une feuille de calcul qui fournit ou contient des informations destinées à être utilisées comme élément probant, l'auditeur a conclu que, bien que les contrôles concernant la saisie des données et ceux sur l'accès à la feuille de calcul aient été adéquatement conçus et qu'ils fonctionnaient efficacement, les contrôles gérant la modification des formules contenues dans la feuille de calcul ne sont pas suffisants. À des moments appropriés tout au long de la période d'audit, l'auditeur pourrait utiliser des outils ou techniques automatisés pour valider de façon indépendante les données générées par la feuille de calcul.

Lorsqu'il n'y a pas de CGI de remplacement ou qu'il n'est pas possible de concevoir des procédures de corroboration adaptées pour répondre aux risques découlant du recours à l'informatique, il se peut que l'auditeur ne soit pas en mesure de s'appuyer sur :

- l'efficacité du fonctionnement des contrôles automatisés dans l'application concernée, sans obtenir d'éléments probants suffisants et directs quant au fait que les contrôles automatisés pertinents ont fonctionné efficacement tout au long de la période d'audit (car il se peut que les CGI ne permettent pas de prévenir ou de détecter de manière appropriée les cas où il y a eu modification des programmes ou accès aux applications sans autorisation);
- l'exhaustivité, l'exactitude et la validité des rapports générés par le système, ou autrement générés en interne par le client de services d'audit, ou des données du client reçues sous forme électronique qui sont utilisés aux fins d'audit, et celles des contrôles manuels reposant sur des

TI qui s'appuient sur de tels rapports ou de telles données (car l'intégrité des informations ainsi communiquées pourrait être compromise);

- l'efficacité du fonctionnement des contrôles sur les entrées de données (car il se pourrait que l'application n'atténue pas suffisamment le risque que des modifications erronées soient apportées, intentionnellement ou non, aux données après leur saisie dans le système). Cela peut également avoir une incidence sur les procédures analytiques de corroboration qui reposent sur des données à un moment précis et que l'auditeur pourrait avoir prévu de mettre en œuvre.

Lorsqu'il évalue l'incidence d'une conception ou d'une mise en place non adéquate d'un CGI, l'auditeur peut, en plus de se poser les questions susmentionnées, se demander :

- s'il est nécessaire de réviser, en application du paragraphe 37 de la norme NCA 315, son évaluation des risques d'anomalies significatives pour tenir compte des nouvelles informations obtenues sur l'efficacité du fonctionnement des contrôles;
- dans le cas où il a relevé au moins une déficience du contrôle interne, si cette déficience est importante et s'il est donc tenu de la signaler aux responsables de la gouvernance, en application de la norme NCA 265, *Communication des déficiences du contrôle interne aux responsables de la gouvernance et à la direction*.

Le fait que l'auditeur en vienne à déterminer, en application du paragraphe 33 de la norme NCA 315, que les procédures de corroboration ne peuvent fournir à elles seules des éléments probants suffisants et appropriés pour répondre à un risque et qu'il n'est pas possible de mettre en œuvre des procédures de remplacement pourrait avoir une incidence sur sa capacité à obtenir des éléments probants suffisants et appropriés et sur son opinion d'audit.

Question 8 – Les CGI sont-ils pertinents si j'adopte une stratégie de corroboration?

Comme il est indiqué ci-dessus, on ne peut acquérir une compréhension des aspects du système d'information qui sont pertinents pour la préparation des états financiers sans avoir d'abord compris les processus informatiques de gestion des accès, de la modification des programmes et des opérations informatiques. Les CGI font eux aussi partie des contrôles sur les processus informatiques de l'entité.

De plus, les CGI sont importants, car ils visent à répondre aux risques découlant du recours à l'informatique, c'est-à-dire les risques liés à l'exhaustivité, à l'exactitude et à la validité des informations se trouvant dans le système d'information de l'entité. (Voir la question 4, qui porte sur les tests de l'efficacité du fonctionnement des CGI.)

Il demeure approprié pour l'auditeur qui adopte une stratégie de corroboration de tenir compte des CGI, car ils lui permettent d'évaluer la conception des contrôles relatifs aux processus et de déterminer si ces contrôles ont été mis en place. L'auditeur peut donc trouver pertinent de tester l'efficacité du fonctionnement des CGI même s'il a l'intention de mettre en œuvre des procédures de corroboration en réponse à un risque.

Par exemple, lorsque l'auditeur a l'intention d'utiliser comme éléments probants, dans le cadre de ses procédures de corroboration, des informations produites par l'entité (rapports générés par le système, données du client reçues sous forme électronique) et que ces informations sont générées par une application, il peut prévoir de tester les contrôles du traitement de l'information dans cette application afin de s'assurer de l'exhaustivité et de l'exactitude des informations, ce qui comprend notamment d'identifier et de tester les CGI visant à répondre aux risques découlant du recours à l'informatique (tels que les risques de modification non autorisée ou inappropriée des programmes, voire des données sous-tendant les rapports).

Parfois, du fait de la complexité du système, l'auditeur ne sera pas en mesure de tester l'exhaustivité et l'exactitude des rapports générés par le système ou des données du client reçues en format électronique au moyen de procédures de corroboration. L'auditeur devrait alors se demander s'il serait plus efficient de tester les contrôles du traitement de l'information et les CGI connexes.

Qu'il prévoie ou non de tester l'efficacité du fonctionnement des contrôles, l'auditeur est tenu, selon le paragraphe 26 de la norme NCA 315, d'acquérir une compréhension de la composante « activités de contrôle », ce qui peut l'amener à évaluer la conception d'un CGI et à déterminer s'il a été mis en place. Voir la question 3 pour des exemples d'éléments à prendre en considération en pareil cas.

Question 9 – Quels sont les éléments à prendre en considération lorsque l'entité fait appel à un tiers relativement à la fourniture de services qui font partie intégrante de son système d'information pertinent pour la préparation des états financiers?

Il est important pour l'auditeur d'acquérir une compréhension suffisante lui permettant de déterminer si l'entité auditée a recours à un tiers fournisseur de services dans le cadre de ses activités. Ce tiers peut ou non être considéré comme une société de services pour l'entité auditée, selon la façon dont l'entité interagit avec lui.

Pour acquérir une compréhension du système de contrôle interne de l'entité conformément à la norme NCA 315, l'auditeur doit identifier, au sein de l'entité, les contrôles de la composante « activités de contrôle » qui ont rapport aux prestations fournies par la société de services, y compris ceux auxquels sont soumises les opérations traitées pour l'entité par la société de services. Il doit aussi évaluer la conception de ces contrôles et déterminer s'ils ont été mis en place[10]. Voir la nouvelle foire aux questions publiée par CPA Canada pour d'autres exemples d'éléments à prendre en considération en ce qui concerne la norme NCA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*.

10 Norme NCA 402, paragraphe 10.

À propos du présent document

La division Recherche, orientation et soutien de Comptables professionnels agréés du Canada (CPA Canada) entreprend des initiatives visant à aider les professionnels en exercice et leurs clients à mieux comprendre les normes et à les mettre en œuvre. Pour identifier les enjeux liés à la mise en œuvre des Normes canadiennes d'audit (NCA) et élaborer des indications de mise en œuvre ne faisant pas autorité relativement à ces enjeux, elle s'appuie sur les conseils du Groupe consultatif sur la mise en œuvre des Normes canadiennes d'audit. Ce dernier a été mis sur pied par CPA Canada et est constitué de bénévoles provenant des cabinets canadiens suivants : BDO, Deloitte, EY, Grant Thornton, KPMG, MNP et PwC.

Le contenu de la présente publication a été élaboré et révisé par divers bénévoles, dont les membres du Groupe consultatif sur la mise en œuvre des Normes canadiennes d'audit de CPA Canada ainsi que des membres du CNAC et de son personnel technique. CPA Canada tient à remercier les bénévoles pour leur soutien lors de la préparation de la FAQ.

Commentaires

Dans une démarche d'amélioration continue et d'élaboration d'indications ne faisant pas autorité de haute qualité, nous aimerions recevoir vos commentaires, questions ou suggestions au sujet de la présente foire aux questions. Veuillez les faire parvenir à :

Yasmine Hakimpour, CPA, CA
Directrice de projets, Audit et certification
Recherche, orientation et soutien
Comptables professionnels agréés du Canada
277, rue Wellington Ouest
Toronto (Ontario) M5V 3H2
Courriel : recherche@cpacanada.ca