



## Le système informatique de l'entité dans la démarche d'audit

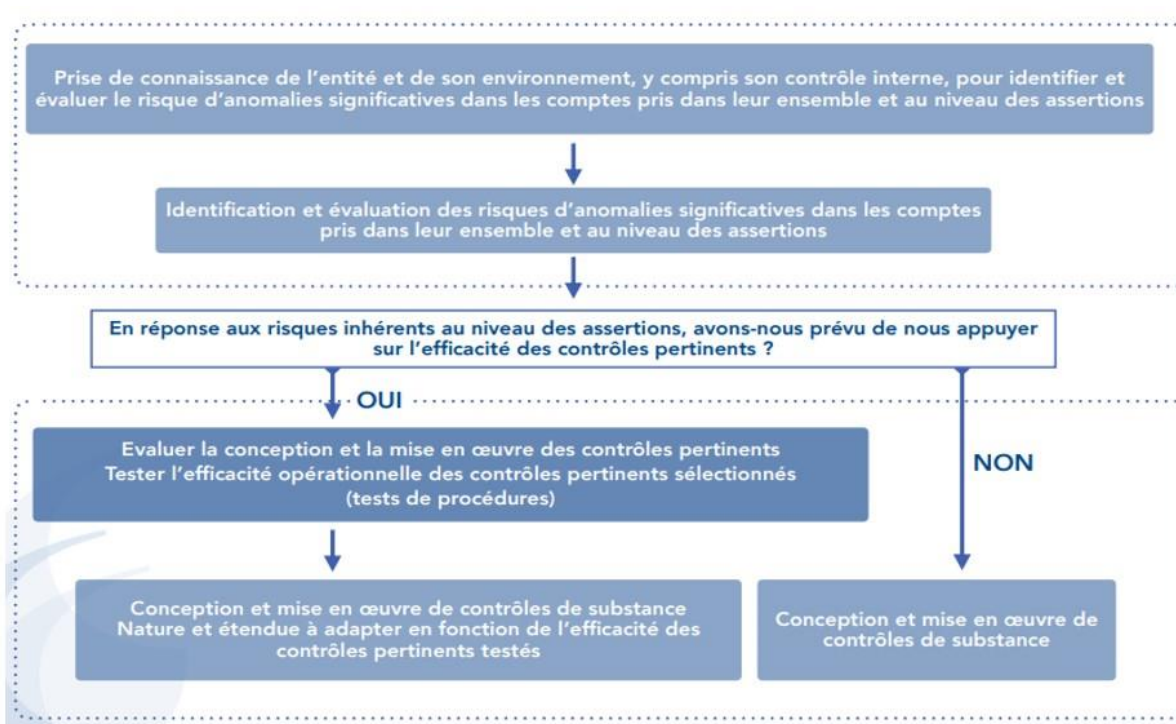
*par Marie-Cécile Moinier et Véronique Collard*

*Temps de lecture estimé : 8 minutes*

Si en application de la NEP 315, le commissaire aux comptes sait pertinemment qu'il doit prendre connaissance du système d'information relatif à l'élaboration de l'information financière de l'entreprise audité, le degré d'implication dans cette démarche est parfois mal appréhendé, notamment sur le volet informatique. Aussi, la Compagnie nationale des commissaires aux comptes a souhaité publier un guide pratique<sup>1</sup> afin de préciser les diligences attendues de la part de l'auditeur légal.

### **Schéma général de la démarche d'audit**

Pour rappel, le commissaire aux comptes doit prendre connaissance des éléments du contrôle interne de l'entité qui contribue à prévenir les risques d'anomalies significatives dans les comptes pris dans leur ensemble, mais aussi au niveau des assertions. À ce titre, il s'informe sur les procédures informatisées ou manuelles mises en place par l'entité pour traiter les opérations ayant un caractère significatif pour les comptes (pris dans leur ensemble) ainsi que sur les enregistrements comptables correspondants. Le système d'information, dont le système informatique est une composante, fait donc partie des éléments du contrôle interne que le commissaire aux comptes intègre dans sa démarche d'audit. Celle-ci est présentée dans le schéma suivant :



Source : CNCC

## La prise de connaissance de l'environnement de contrôle informatique

L'objectif de cette première phase est de comprendre les processus informatiques en lien avec la production de l'information financière. Pour ce faire, le commissaire aux comptes va s'attacher à obtenir des informations sur :

- l'organisation et la gouvernance de la fonction informatique (notamment centralisation ou non de la fonction) ;
- le degré de connaissance des risques informatiques et les actions mises en place pour y remédier (ex. cybersécurité) ;
- les applications utilisées en lien avec la production de l'information financière ;
- le recours, le cas échéant, à la sous-traitance informatique ;
- la gestion du système informatique (gestion des accès, changement applicatif, adéquation du système avec l'évolution de l'entité, etc.).

Lors de ses diligences, le commissaire aux comptes peut être amené à rencontrer plusieurs facteurs de risques.

### Exemple de facteurs de risques

- un sous-dimensionnement de la fonction informatique,
- une absence de séparation des fonctions au sein des processus informatiques,
- une maîtrise insuffisante des risques informatiques (risque cyber, non-respect d'obligations légales [RGPD, conformité du FEC], insuffisance des sauvegardes.

## **Évaluer les processus clés dans la démarche d'identification du risque d'anomalies significatives dans les comptes**

Dans le prolongement de la phase exposée ci-avant, le commissaire aux comptes va ensuite approfondir sa connaissance sur les processus clés de l'entité (ex. processus de vente, d'achat ou de gestion des stocks).

Dans sa démarche, le commissaire aux comptes cherche notamment à identifier les points suivants :

- le respect du principe de séparation des tâches,
- les applications / outils bureautiques supportant le flux d'informations,
- les documents/données sources et les fichiers utilisés dans le processus,
- les états et fichiers générés dans le processus,
- la complexité des traitements informatiques, la volumétrie des transactions réalisées,
- les éventuelles interfaces utilisées entre les applications.

### **Remarque**

La restitution de ces informations sous forme de diagramme de flux permet une visualisation synthétique du cheminement des opérations et des flux.

En fonction des résultats obtenus lors de ces deux phases et en fonction de l'approche qu'il décide de retenir, le commissaire aux comptes peut décider de s'appuyer sur les contrôles mis en place par l'entité. Dans ce cadre, il doit alors s'assurer de leur efficacité en les testant.

### **Tester les procédures de l'entité**

Les diligences vont essentiellement se diriger sur les contrôles généraux informatiques (Information Technology Général Controls ou ITGC), sur les contrôles portés par les applications, plus ou moins automatisés (Information Technology Application Control ou ITAC) ainsi que les informations produites par l'entreprise (IPE) qui participent indirectement à l'élaboration des états financiers.

## **Tests sur les contrôles généraux informatiques (ITGC)**

Rappelons qu'un environnement informatique comprend des applications, point d'entrée des utilisateurs métiers, une base de données (ex. liste des fournisseurs à date), un système d'exploitation et un réseau permettant d'échanger des informations en interne et en externe.

Les principaux risques relatifs à cet environnement portent sur les points suivants :

- la gestion des accès (niveau d'autorisation pour les créations et modifications des accès, mots de passe pas assez robustes, désactivation trop longue pour des salariés ayant quitté l'entreprise) ;
- la gestion des changements (sur les applications, les modifications de paramètres, voire changement de système d'exploitation) insuffisamment testés et validés avant mise en services ;
- la gestion de l'exploitation informatique (incidents non répertoriés ou résolus de manière inappropriée) ;
- la gestion des projets informatiques (projet surdimensionné ou sous-dimensionné par rapport aux caractéristiques de l'entité, insuffisance des tests avant mise en service, problématique liée à la migration des données, etc).

Après avoir évalué la conception et la mise en œuvre des contrôles réalisés par l'entité, le commissaire aux comptes va sélectionner les contrôles pertinents pour son audit et qu'il souhaite tester. Cette démarche a pour objectif de vérifier que les contrôles sont réalisés selon les modalités prévues, aux moments adéquats, de façon constante tout au long de la période contrôlée et par la bonne personne et/ou le bon processus.

### **Important !**

Le commissaire aux comptes doit s'assurer que les ITGC couvre l'ensemble de l'exercice audité. Si ce n'est pas le cas ou lorsque des changements sont intervenus, il peut être conduit à collecter des éléments complémentaires et/ou réaliser des procédures additionnelles pour évaluer l'efficacité des contrôles sur toute la période audité.

Si les tests effectués sur le ITGC ne révèlent aucun dysfonctionnement, le commissaire en tient compte dans sa démarche d'audit, notamment s'il décide de réaliser des tests sur les contrôles applicatifs et sur l'intégrité des informations produites par l'entité.

En cas de faiblesse constatée sur les ITGC, le commissaire aux comptes doit s'interroger sur son impact pour les contrôles applicatifs qu'il souhaitait tester.

## **Tests sur les contrôles applicatifs (ITAC)**

On recense plusieurs types d'ITAC, qu'ils soient directement intégrés dans des solutions logicielles (ERP) ou élaborés en interne. Ils peuvent être entièrement automatisés ou avoir aussi une composante manuelle.

### **Exemple d'ITAC**

- processus « achat » : contrôle du rapprochement commande/livraison/facturation.
- contrôle d'accès pour réaliser certaines tâches (par ex. modification des prix de vente).
- contrôle d'interface visant à garantir l'exhaustivité des flux (ex. remontée des encaissements sur logiciels de caisse vers la comptabilité générale).

En premier lieu, le commissaire aux comptes va s'intéresser à la conception des contrôles automatisés, notamment aux règles de paramétrage, à l'existence de seuil de déclenchement des contrôles, au périmètre des entités/transactions concernées, à la fréquence des contrôles, etc. Lorsqu'il estime que la conception est satisfaisante, il vérifie alors que les contrôles sont correctement mis en œuvre.

Dans la mesure où les tests sur les ITGC ont été concluants et qu'il en est de même pour l'évaluation de la mise en œuvre des ITAC sélectionnés, le commissaire peut s'abstenir de procéder à des tests sur ces derniers. Néanmoins, s'il cherche à couvrir des risques spécifiques, il peut réaliser des tests de procédures, tels que par exemple sur la restriction des accès aux personnes autorisées à modifier le paramétrage de l'application.

## **Tests sur la fiabilité des informations produites par l'entité (IPE)**

Notons qu'il ne s'agit pas des états comptables constituant la comptabilité de l'entité, mais des informations produites par des applications informatiques ou des outils qui concourent à l'élaboration des états financiers.

### **Exemple d'IPE**

- rapport d'anomalies pour des factures bloquées au paiement.
- la liste des nouveaux employés en corrélation avec la création des dossiers « salariés ».
- la balance âgée servant de base aux dépréciations des comptes clients.

Dans sa démarche, le commissaire aux comptes cherche à identifier les risques liés à l'entrée et au traitement des données, ainsi que ceux liés à l'extraction et à la manipulation des données. Pour ce faire, il peut effectuer des tests de procédures mais aussi des contrôles de substance en collectant des éléments probants sur la fiabilité de l'IPE.

## Point particulier : externalisation de la fonction informatique

Lors de sa prise de connaissance de l'environnement informatique, le commissaire peut constater que l'entité a opté pour une délégation (pour tout ou partie) de son service informatique (par ex. application en mode SaaS). Dans cette hypothèse, le commissaire aux comptes peut s'appuyer, le cas échéant sur un rapport d'assurance (de type ISAE 3402) comportant une description et la conception des contrôles mis en œuvre par le prestataire (type I), voire de type II, qui en sus comporte un volet « efficacité des contrôles » mis en œuvre par le prestataire.

### Pour conclure

La place de la revue du système informatique dans la démarche du commissaire aux comptes prendra une dimension variable propre à chaque entité auditée. Le choix des diligences par le commissaire aux comptes doit être sagement mesuré et argumenté pour que la démarche de revue des systèmes informatiques soit correctement dimensionnée à chaque entreprise et soit utilement mis au service de la mission de certification des comptes. En espérant que les fiches et les outils mis à disposition de la profession permettent d'avoir recours à un ou plusieurs domaines d'analyse, après une phase de prise de connaissance qui reste toujours une brique indispensable à mettre en œuvre.

<sup>1</sup> CNCC, « Le système informatique dans la démarche d'audit », février 2023.