Le système **informatique** dans la démarche **d'audit**

Fiches pratiques

Février 2023

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

Le système **informatique** dans la démarche **d'audit**

Fiches pratiques

FICHES AUDIT SI

Février 2023

Le système informatique dans la démarche d'Audit

Présentation

Dans le cadre de sa mission de certification des comptes et en application de la « *NEP 315 – Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives* », le commissaire aux comptes acquiert une connaissance suffisante de l'entité, y compris des éléments du contrôle interne pertinents pour l'audit dont le système d'information relatif à l'élaboration de l'information financière (cf. extrait de la NEP 315 en annexe – Références normatives).

Le système d'information comprend des traitements informatisés, assurés par le système informatique, et des traitements manuels. Le système informatique est donc une composante du système d'information.

La présente collection de fiches techniques «Le système informatique dans la démarche d'audit » a pour objectifs de décliner par thématiques la prise en compte du système informatique, par le commissaire aux comptes, dans les différentes étapes de sa mission de certification des comptes et de proposer des outils pratiques pour la mise en œuvre de ses diligences.

Les autres aspects du système d'information (autre que la composante informatique) sont présentés dans la note d'information « NI XV. Le commissaire aux comptes et l'approche d'audit par les risques » à laquelle le commissaire aux comptes peut utilement se référer.

Par ailleurs, la prise en compte de l'environnement informatique lors de l'audit des comptes ne doit pas être confondue avec l'audit informatique d'un système d'information confié à un commissaire aux comptes dans le cadre des prestations en dehors d'une mission légale et pouvant prendre la forme d'un diagnostic.

La démarche d'audit retenue par le commissaire aux comptes sur le système informatique en lien avec la production de l'information comptable ne diffère pas de celle mise en œuvre sur les autres aspects de sa mission de certification, à savoir :

- L'identification et l'évaluation du risque d'anomalies significatives dans les comptes ;
- La conception des réponses à ce risque.

I- Identification et évaluation des risques d'anomalies significatives dans les comptes liés à l'environnement de contrôle informatique

Pour identifier et évaluer le risque d'anomalies significatives dans les comptes, le commissaire aux comptes prend obligatoirement connaissance de l'entité et de son environnement, y compris de son contrôle interne dont le système d'information relatif à l'élaboration de l'information financière.

Le système d'information se compose :

- De l'infrastructure technique (équipements et matériels informatiques tels que les serveurs, pare-feux, routeurs, salles informatiques hébergeant les systèmes, …) ;
- De logiciels et/ou progiciels et des interfaces inter-applications ;
- De personnel nécessaire à la maintenance du service informatique (personnel technique et fonctionnel interne à la société et/ou prestataires) ;
- De procédures et de données. Les procédures doivent être conçues de façon à, notamment, permettre de centraliser les informations des différents systèmes de traitement des opérations au grand livre.

Les systèmes informatiques sur lesquels s'appuient ces systèmes d'information doivent être protégés afin d'assurer la conservation des informations stockées.

La connaissance du système informatique, par le commissaire aux comptes, peut s'appuyer sur la revue de la documentation disponible dans l'entité et/ou sur des demandes d'information au moyen d'entretiens avec la direction des systèmes d'information (DSI) dans certaines entités de taille significative ou avec tout interlocuteur dans des entités de plus petite taille.

Pour ce faire, le commissaire aux comptes prend connaissance :

- De l'environnement de contrôle informatique : **Fiche n°1 • Prise de connaissance de l'environnement de contrôle informatique / Outil n°1 : Papier de travail sur la prise de connaissance de l'environnement de contrôle informatique ;**
- Des processus clés de l'entité, en particulier des systèmes informatiques sous-jacents, ayant un impact direct ou indirect sur les comptes significatifs et les informations significatives fournies en annexe : **Fiche n°2 • Compréhension des processus et des systèmes informatiques sous-jacents pertinents pour l'audit / Outil n°2 : Exemple de formalisation des processus clés**.

Cette prise de connaissance permet au commissaire aux comptes :

- d'apprécier l'importance du système informatique sur l'évaluation du risque d'anomalies significatives sur les comptes pris dans leur ensemble et au niveau des assertions et,
- de définir sa stratégie d'audit, autrement dit, s'il a l'intention de s'appuyer ou non sur les contrôles de l'entité.

Selon la taille et la complexité des systèmes informatiques, le commissaire aux comptes peut décider, à l'issue de cette étape, de faire appel à un auditeur spécialisé dans les systèmes informatiques notamment s'il estime que des compétences informatiques particulières sont nécessaires pour réaliser la mission. Dans ce cas, le commissaire aux comptes applique la *NEP 620 – Intervention d'un expert*.

II- Réponse aux risques identifiés

En pratique, les interlocuteurs étant les mêmes, lors de la prise de connaissance des systèmes informatiques, le commissaire aux comptes va également prendre connaissance des procédures de contrôle interne mises en œuvre en réponse aux risques liés aux systèmes informatiques. C'est pourquoi, les diligences à mettre en œuvre par le commissaire aux comptes figurent en fiche n°2 précédemment citée.

Un audit ne requiert pas systématiquement de tester tous les contrôles de l'entité. En effet, le commissaire aux comptes évalue la conception et la mise en œuvre de ces contrôles pour l'audit lorsqu'il :

- a identifié un risque significatif, quand bien même il ne souhaiterait pas s'appuyer sur ces contrôles (cas obligatoire indépendamment de la stratégie d'audit) ,
- considère que les contrôles de substance seuls ne permettront pas d'obtenir les éléments suffisants et appropriés pour conclure (cas obligatoire indépendamment de la stratégie d'audit) ,
- souhaite s'appuyer sur les contrôles de l'entité pour réduire le risque d'anomalies significatives et/ou pour limiter l'étendue des contrôles de substance à mettre en œuvre.

Concernant le système informatique, lorsque le commissaire aux comptes s'appuie sur les contrôles de l'entité, il peut mettre en œuvre :

- Des tests sur les contrôles généraux informatiques, appelés également *Information Technology General Control* – ITGC : **Fiche n°3 • Les contrôles généraux informatiques - ITGC / Outil n°3 : Liste des contrôles généraux informatiques – ITGC** ;
- Des tests sur les contrôles portés par les applications, appelés également *Information Technology Application Control* – ITAC : **Fiche n°4 • Les contrôles applicatifs – ITAC / Outil n°4 : Evaluation des contrôles applicatifs – ITAC** ;
- Des tests sur les informations produites par l'entité – IPE : **Fiche n°5 • Les informations produites par l'entité – IPE / Outil n° 5 Appréciation de la fiabilité des IPE**.

Par ailleurs, l'externalisation d'une fonction informatique est une solution qui est de plus en plus fréquemment utilisée par les entreprises. Le commissaire aux comptes met alors en

œuvre des procédures d'audit, y compris lorsque ces procédures sont déléguées à des prestataires de services externes : **Fiche n°6 • Prise en compte d'une délégation de services informatiques dans l'approche d'audit**[1] **/ Outil n°6 : Papier de travail – Appréciation du rapport d'assurance relatif au dispositif de contrôle interne mis en oeuvre par un prestataire dans le cadre d'une délégation de service**.

(1) Cette fiche porte sur les délégations de services informatiques et ne traite donc pas de tous les cas de délégations de services pouvant exister dans l'entité auditée (par exemple, pour la gestion de la paie). Pour les cas particuliers de centres de services partagés, se référer à la Note d'information XIX - Le commissaire aux comptes et l'audit d'une entité ayant recours aux services d'un centre de services partagés au sein d'un groupe.

Les contrôles généraux informatiques ou ITGC

Pour s'assurer que les éléments de l'environnement informatique (applications, bases de données, ...) fonctionnent comme attendu, l'entité met en place des processus de gestion des systèmes informatiques qui permettent de répondre aux risques que l'environnement informatique ne fonctionne pas comme prévu.

Les contrôles généraux informatiques (ITCG) sont des contrôles mis en place par l'entité sur ces processus de gestion des systèmes informatiques pour s'assurer qu'ils atteignent leur objectif. Ils assurent que les contrôles liés au système informatique fonctionnent correctement tel que prévu, et tout au long de l'année.

Lorsque le commissaire aux comptes s'appuie sur les contrôles généraux informatiques, il met en œuvre des diligences relatives à la gestion des accès, des changements, de l'exploitation informatique et des projets informatiques, s'il estime pertinent .

Les contrôles portés par les applications informatiques ou ITAC

Lors de la prise de connaissance des processus clés (par exemple, le processus des ventes, le processus des achats, le processus des stocks, ...), le commissaire aux comptes a identifié des contrôles de l'entité pertinents pour l'audit dont certains sont automatisés ou manuels avec une composante informatique.

Ces contrôles automatisés ou mixtes (c'est-à-dire intégrant une composante automatisée et une composante manuelle) portés par les applications informatiques sont dénommés ITAC.

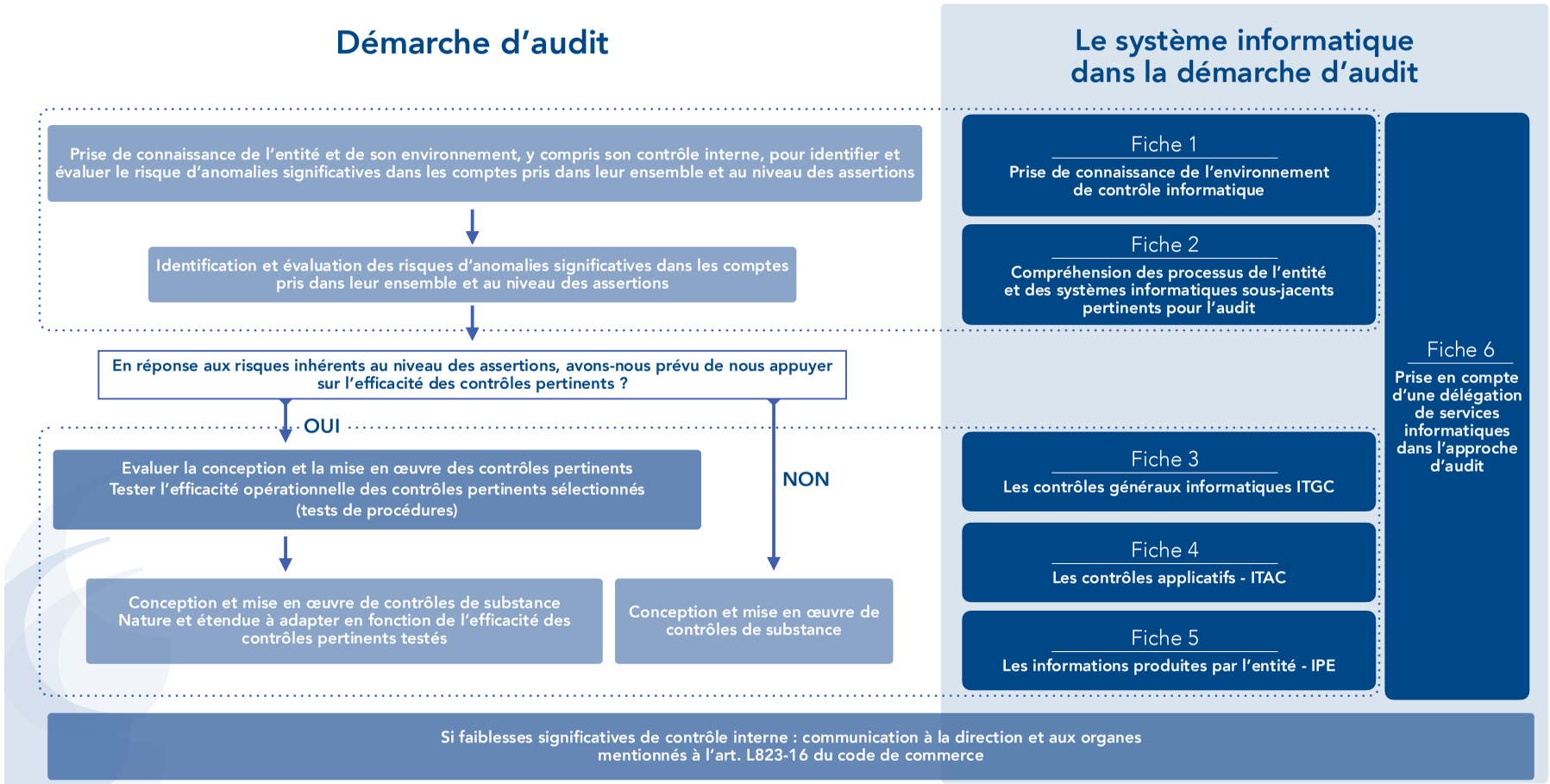
Lorsque la stratégie d'audit retenue par le commissaire aux comptes repose sur ces ITAC, il s'assure que ces derniers fonctionnent comme prévu tout au long de l'exercice audité. Pour ce faire, il peut s'appuyer sur les tests réalisés sur les ITGC (cf. ci-dessus), lesquels permettent de s'assurer de la fiabilité et de la stabilité des ITAC concernés sur la période, ou le cas échéant, il peut mettre en œuvre des procédures alternatives afin de vérifier la stabilité de ces ITAC tout au long de l'exercice.

Les informations produites par l'entité ou IPE

Les IPE représentent toutes les informations produites par l'entité que le commissaire aux comptes peut être amené à utiliser dans le cadre de ses procédures d'audit, qu'elles soient produites par les applications informatiques, des outils tels que Word ou Excel (appelés plus généralement "outils bureautiques"), ou par tout autre moyen, y compris manuellement.

Dans ce cas, le commissaire aux comptes apprécie la fiabilité des informations produites par l'entité (IPE) sur lesquelles il a l'intention de s'appuyer pour la réalisation de certaines procédures d'audit.

Les travaux du commissaire aux comptes relatifs au système informatique font partie intégrante de sa démarche d'audit et sont présentés dans le **schéma suivant** :


Démarche d'audit
Le système informatique dans la démarche d'audit
Prise de connaissance de l'entité et de son environnement, y compris son contrôle interne, pour identifier et évaluer le risque d'anomalies significatives dans les comptes pris dans leur ensemble et au niveau des assertions
Identification et évaluation des risques d'anomalies significatives dans les comptes pris dans leur ensemble et au niveau des assertions
En réponse aux risques inhérents au niveau des assertions, avons-nous prévu de nous appuyer sur l'efficacité des contrôles pertinents ?
OUI
NON
Evaluer la conception et la mise en œuvre des contrôles pertinents
Tester l'efficacité opérationnelle des contrôles pertinents sélectionnés (tests de procédures)
Conception et mise en œuvre de contrôles de substance
Nature et étendue à adapter en fonction de l'efficacité des contrôles pertinents testés
Conception et mise en œuvre de contrôles de substance
Si faiblesses significatives de contrôle interne : communication à la direction et aux organes mentionnés à l'art. L823-16 du code de commerce
Fiche 1
Prise de connaissance de l'environnement de contrôle informatique
Fiche 2
Compréhension des processus de l'entité et des systèmes informatiques sous-jacents pertinents pour l'audit
Fiche 3
Les contrôles généraux informatiques ITGC
Fiche 4
Les contrôles applicatifs - ITAC
Fiche 5
Les informations produites par l'entité - IPE
Fiche 6
Prise en compte d'une délégation de services informatiques dans l'approche d'audit

Références normatives

V.I. NEP 315
Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives

La prise de connaissance du système d'information est une obligation puisqu'elle fait partie des éléments listés par la norme 315 §14 :

« La prise de connaissance des éléments du contrôle interne pertinents pour l'audit permet au commissaire aux comptes d'identifier les types d'anomalies potentielles et de prendre en considération les facteurs pouvant engendrer des risques d'anomalies significatives dans les comptes.

Le commissaire aux comptes prend connaissance des éléments du contrôle interne qui contribuent à prévenir le risque d'anomalies significatives dans les comptes, pris dans leur ensemble et au niveau des assertions.

Pour ce faire, le commissaire aux comptes prend notamment connaissance des éléments suivants :

- *[…]*
- *le système d'information relatif à l'élaboration de l'information financière. A ce titre, le commissaire aux comptes s'intéresse notamment :*
- *aux catégories d'opérations ayant un caractère significatif pour les comptes pris dans leur ensemble ;*
- *aux procédures, informatisées ou manuelles, qui permettent d'initier, enregistrer et traiter ces opérations et de les traduire dans les comptes ;*
- *aux enregistrements comptables correspondants, aussi bien informatisés que manuels ;*
- *à la façon dont sont traités les événements ponctuels, différents des opérations récurrentes, susceptibles d'engendrer un risque d'anomalies significatives ;*
- *au processus d'élaboration des comptes, y compris des estimations comptables significatives et des informations significatives fournies dans l'annexe des comptes ;*
- *la façon dont l'entité communique sur les éléments significatifs de l'information financière et sur les rôles et les responsabilités individuelles au sein de l'entité en matière d'information financière. A ce titre, le commissaire aux comptes s'intéresse notamment à la communication entre la direction et les organes mentionnés à l'article L. 823-16 du code de commerce ou les autorités de contrôle ainsi qu'aux actions de sensibilisation de la direction envers les membres du personnel afin de les informer quant à l'impact que peuvent avoir leurs activités sur l'élaboration de l'information financière. »*

Références normatives

V.I. NEP 330
Procédures d'audit mises en oeuvre par le commissaire aux comptes à l'issue de son évaluation des risques

5. En réponse à son évaluation du risque au niveau des assertions, le commissaire aux comptes conçoit et met en œuvre des procédures d'audit complémentaires à celles réalisées pour cette évaluation.

Ces procédures d'audit comprennent des tests de procédures, des contrôles de substance, ou une approche mixte utilisant à la fois des tests de procédures et des contrôles de substance.

Le commissaire aux comptes détermine la nature, le calendrier et l'étendue des procédures d'audit qu'il réalise en mettant en évidence le lien entre ces procédures d'audit et les risques auxquels elles répondent.

Références normatives

Note d'information CNCC XV
Le commissaire aux comptes et l'approche d'audit par les risques

La note d'information de la CNCC consacrée à l'approche par les risques aborde la définition et l'importance du système d'information sur la détermination de l'approche par les risques.

Extrait de l'annexe 2 de la NI Approche (= traduction de l'ISA 315) :

« Système d'information relatif à l'élaboration de l'information financière et à sa communication :

Un système d'information se compose de l'infrastructure (équipements et matériel informatique), de logiciels, du personnel, de procédures et de données. Beaucoup de systèmes d'information font un appel intensif à un système informatique.

Le système d'information répondant aux objectifs d'élaboration de l'information financière, qui comprend le système d'établissement des états financiers, couvre des méthodes et des documents qui :

- *identifient et enregistrent toutes les opérations valides ;*
- *décrivent en temps voulu les opérations avec suffisamment de détails afin d'en permettre la classification correcte pour l'établissement des états financiers ;*
- *évaluent les transactions de façon à permettre leur enregistrement dans les états financiers à la valeur monétaire appropriée ;*
- *déterminent quand les opérations ont eu lieu afin de pouvoir les enregistrer dans la période comptable appropriée ;*
- *présentent correctement les opérations dans les états financiers ainsi que les informations à fournir les concernant. »*

Retrouvez les normes d'exercice professionnel et les notes d'information **sur SIDONI**

Fiche n°1

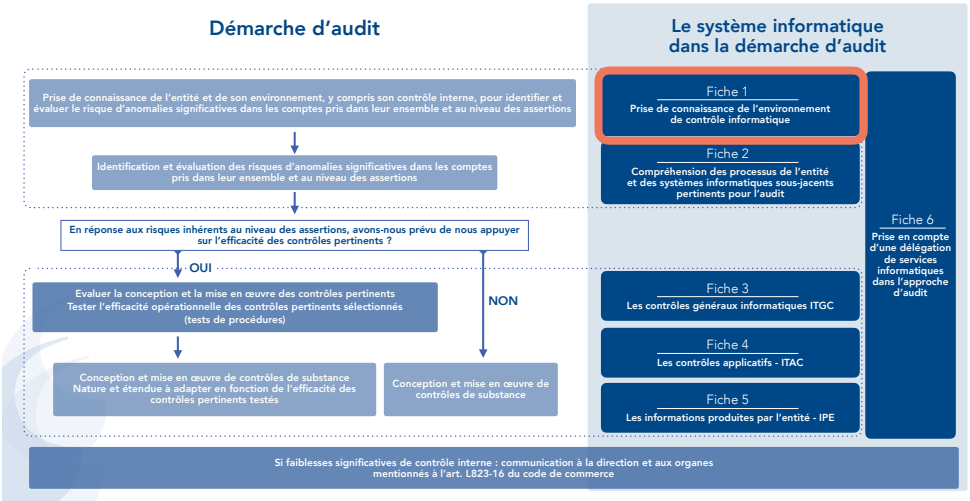
Prise de connaissance de l'environnement de contrôle informatique

Retour Sommaire

I - Position dans la démarche d'audit

Le système d'information dont le système informatique est une composante, fait partie des éléments du contrôle interne pertinents pour l'audit dont prend connaissance le commissaire aux comptes en vue d'évaluer le risque d'anomalies significatives dans les comptes et en déduire son approche d'audit.

La fiche n°2 « Compréhension des processus de l'entité et des systèmes informatiques sous-jacents pertinents pour l'audit » aborde de manière plus détaillée la description des processus clés et en particulier des systèmes informatiques sous-jacents.



Un **exemple de papier de travail** est proposé en annexe de cette fiche permettant de **documenter la prise de connaissance de l'environnement de contrôle informatique** par le commissaire aux comptes.

NEP 315
Prise de connaissance

NI XV
Approche par les risques

II - Objectifs

Les objectifs de cette fiche sont de guider le commissaire aux comptes dans :

- ☑ la compréhension des systèmes informatiques en lien avec la production de l'information financière,
- ☑ l'identification des risques d'anomalies significatives liés à l'environnement de contrôle informatique,
- ☑ l'appréciation de l'environnement de contrôle informatique mis en place par l'entité pour réduire ces risques.

III - Diligences du commissaire aux comptes

Prise de connaissance générale des systèmes informatiques de l'entité

Lors de sa prise de connaissance des éléments du contrôle interne pertinents pour l'audit, le commissaire aux comptes prend notamment connaissance des systèmes informatiques, en lien avec la production de l'information financière, qui intègrent les éléments suivants :

Organisation et gouvernance de la **fonction informatique**	Identification des **risques informatiques** par l'entité (dont le risque cybersécurité)
Niveau et périmètre de **sous-traitance**	Liste des applications en lien avec la **production de l'information financière**
Processus relatifs à la **gestion du système informatique** : accès, changement, exploitation et projet	Evolutions du **système d'informations**

Cette prise de connaissance est réalisée principalement par des demandes d'information (entretiens), par observation et par inspection de documents.

Identification des risques d'anomalies significatives liés à l'environnement de contrôle informatique

Les facteurs de risques peuvent être :

- un pilotage insuffisant de la fonction informatique par la gouvernance,
- une dépendance à des prestataires externes non maîtrisée,
- une compétence inadaptée au regard des technologies utilisées,
- un sous-dimensionnement de la fonction informatique,
- une maîtrise insuffisante des projets informatiques,
- la non séparation des fonctions au sein des processus informatiques,
- une maîtrise insuffisante par l'entité des risques informatiques (par exemple le risque lié à la cybersécurité),
- la perte d'intégrité des données,
- la perte de la continuité d'activité (par exemple, insuffisance en matière de gestion des sauvegardes et de plan de reprise d'activité, …),
- le non-respect des obligations légales et réglementaires (RGPD*, FEC*, archivage fiscal, PAF* …),
- etc.

✳ **RGPD** : Règlement général sur la protection des données.
✳ **FEC** : Fichier des écritures comptables.
✳ **PAF** : Piste d'audit fiable.

IV - Incidences sur la démarche d'audit

A l'issue de cette prise de connaissance des systèmes informatiques de l'entité, le commissaire aux comptes est en mesure :

- d'apprécier la qualité de l'environnement de contrôle informatique par la direction de l'entité, la complexité du système d'information, la criticité du système d'information pour la production de l'information financière,
- d'orienter son approche d'audit en fonction des éléments pertinents relevés. Par exemple, il peut :
  - prévoir la réalisation de diligences spécifiques liées à un événement tel qu'un changement de système informatique ou un incident significatif sur une application informatique critique (comme l'incapacité à restaurer une application ou des données ou encore un incident de cybersécurité majeur, etc.),
  - envisager de recourir à l'intervention d'un auditeur spécialisé dans les systèmes informatiques,
  - etc.
- d'identifier, le cas échéant, les faiblesses significatives liées à l'environnement de contrôle informatique et à communiquer par écrit à la direction de l'entité et aux organes de gouvernance, conformément à la NEP 265. S'agissant des autres faiblesses, le commissaire aux comptes apprécie, en fonction de son jugement professionnel, l'opportunité de les communiquer au niveau approprié au sein de l'entité.

Fiche n°2

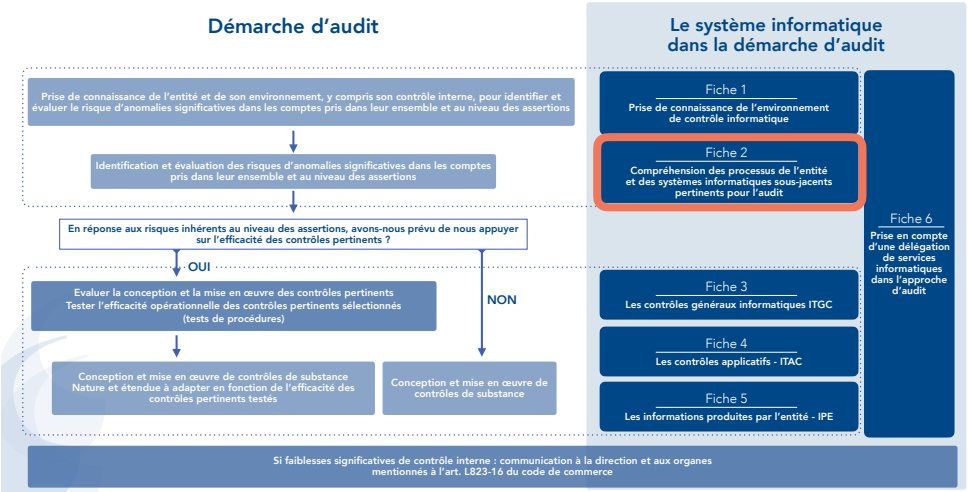
Compréhension des processus de l'entité et des systèmes informatiques sous-jacents pertinents pour l'audit

Retour Sommaire

I - Position dans la démarche d'audit

Après une première prise de connaissance générale des systèmes informatiques de l'entité (cf. fiche n°1), le commissaire aux comptes approfondit sa compréhension des processus clés de l'entité (par exemple, le processus des ventes, le processus des achats, le processus des stocks, ...) pour définir les composants du système informatique sous-jacent pertinents pour l'audit.

En fonction de la stratégie d'audit retenue à la suite de cette prise de connaissance, le commissaire aux comptes définit les procédures d'audit à mettre en œuvre, le cas échéant, sur ces composants (cf. fiches n°3, n°4 et n°5).



Un **exemple de formalisation des processus** sous forme d'un diagramme de flux est proposé en annexe de cette fiche.

NEP 315
Prise de connaissance

NI XV
Approche par les risques

II - Objectifs

Les objectifs de cette fiche sont de guider le commissaire aux comptes en vue :

- ☑ de comprendre les processus clés depuis l'initiation des transactions, jusqu'à leur enregistrement en comptabilité et notamment leur dimension informatique, y compris le degré d'automatisation (procédures automatisées, manuelles ou manuelles avec une composante informatique) et de complexité du système d'information,
- ☑ d'identifier les risques d'anomalies significatives au niveau des assertions en particulier ceux résultant de l'utilisation de systèmes informatiques,
- ☑ d'identifier les contrôles portés par les applications informatiques pertinents pour l'audit sur lesquels le commissaire aux comptes a l'intention de s'appuyer (les contrôles applicatifs –« ITAC(1) » et les états clés issus des applications – « IPE(2) »).

(1) ITAC : Information Technology Application Control.

(2) IPE : Information Produite par l'Entité.

III - Diligences du commissaire aux comptes

Prise de connaissance des procédures de l'entité sur les processus clés

Pour chacun des processus clés (autrement dit ceux contribuant directement ou indirectement à la production des comptes), le commissaire aux comptes prend connaissance [par demandes d'informations (entretiens), par observation, par inspection de documents] des procédures de l'entité et identifie les étapes du flux d'informations qui sont manuelles et celles qui font appel aux systèmes informatiques.

La compréhension des flux d'informations au sein des processus clés couvre les différentes étapes de l'opération, depuis son initiation jusqu'à son enregistrement, son traitement et sa traduction dans les comptes (écriture comptable et mention en annexe) .

En particulier, pour chacune de ces étapes, le commissaire aux comptes cherche à identifier :

- les personnes impliquées et 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 (les informations produites par l'entité - IPE),
- le traitement des données (calculs, traitements batch,...),
- la complexité des traitements informatiques,
- la volumétrie des transactions réalisées,
- les éventuelles interfaces utilisées entre les applications.

Le commissaire aux comptes peut documenter sa prise de connaissance sous forme narrative ou sous la forme d'un diagramme de flux (*flow chart*).

Cette prise de connaissance permet au commissaire aux comptes d'identifier les risques d'anomalies significatives au niveau des assertions.

Identification des risques d'anomalies significatives au niveau des assertions

Ces risques peuvent porter, par exemple, sur :

- L'utilisation d'applications ou entrepôts de données («*data warehouse* ») ou d'outils bureautiques (tableurs, logiciels de bases de données...) :
  - traitant des données mal saisies ou mal interfacées ou non exhaustives, ... ,
  - traitant incorrectement des données (mauvais paramétrage, traitement/calcul erroné),
  - produisant des états inexacts ou incomplets.
- Une mauvaise définition des rôles et responsabilités dans la gouvernance d'une base de données référentielle pouvant générer :
  - la destruction des données ou leur modification inappropriée générant une perte d'intégrité,
  - l'enregistrement d'opérations non autorisées, voire inexistantes,
  - l'enregistrement incorrect des opérations,
  - la possibilité pour le personnel, que ce soit des services informatiques ou métiers, d'obtenir des accès privilégiés (par exemple : administrateur...) au-delà de ceux nécessaires à l'exercice de leur fonction, contrevenant ainsi au principe de séparation des tâches,
  - des changements non autorisés de données dans les fichiers maîtres (par exemple : référentiels fournisseur et client...),
  - des changements non autorisés apportés aux systèmes ou aux programmes informatiques,
  - la non-réalisation des changements nécessaires dans les applications,
  - des interventions manuelles inappropriées,
  - la perte potentielle de données ou l'incapacité à accéder à certaines données (par exemple : restauration des applications, archivage...).

Ces risques sur les systèmes informatiques peuvent avoir des répercussions sur les états financiers.
A titre d'illustrations :

- *La perte potentielle de données de facturation peut engendrer un risque d'anomalies significatives sur l'exhaustivité du chiffre d'affaires ;*
- *L'accès non autorisé aux données peut remettre en cause la réalité des flux de chiffre d affaires.*

Identification des contrôles de l'entité pertinents pour l'audit

Cette prise de connaissance a également pour objectif d'identifier les contrôles de l'entité pertinents pour l'audit[3], qu'ils soient manuels, automatisés ou manuels avec une composante informatique, sur lesquels le commissaire aux comptes peut s'appuyer.

(3) Cf. NI XV
Le commissaire aux comptes et l'approche d'audit par les risques (page 31) sur les aspects relatifs « aux contrôles de l'entité pertinents pour l'audit ».

Seules les deux dernières catégories (automatisés et manuels avec une composante informatique) sont traitées dans la présente collection de fiches techniques « **Le système informatique dans la démarche d'audit** ».

Un contrôle automatisé peut être, par exemple, le rapprochement automatique commande / réception / facture pour le processus achats (communément appelé le « 3 way match »).

Un contrôle manuel avec une composante informatique peut être par exemple :

- *une revue mensuelle des créances clients réalisée par le comptable (composante manuelle) sur la base d'une balance âgée (état issu d'une application constituant la composante informatique - IPE),*
- *une approbation de commande d'achat dans l'application (composante manuelle) déclenchant automatiquement l'envoi à l'approbateur suivant, selon la procédure de validation (composante informatique).*

IV - Incidences sur la démarche d'audit

A l'issue de cette phase de prise de connaissance (de l'environnement de contrôle informatique (fiche n°1) et des processus clés (fiche n°2)), le commissaire aux comptes définit sa stratégie d'audit, autrement dit s'il a l'intention ou non de s'appuyer sur les contrôles de l'entité (communément appelé « approche contrôle »).

Lorsque le commissaire aux comptes s'appuie sur les contrôles de l'entité[4], les diligences à mettre en œuvre peuvent inclure :

- le test des contrôles généraux informatiques – ITGC[5] - sur les applications supportant les contrôles automatisés ou manuels avec une composante informatique ou les IPE (cf. fiche n°3 - Tests des contrôles généraux informatiques – ITGC),
- le test des contrôles automatisés ou manuels avec une composante informatique (cf. fiche n°4 – ITAC),
- le test des IPE (cf. fiche n°5 – IPE).

En fonction des compétences informatiques nécessaires pour la réalisation de ces tests, le commissaire aux comptes apprécie s'il convient de faire appel à un auditeur spécialisé dans les systèmes informatiques.

Le cas échéant, le commissaire aux comptes communique, à l'issue de cette prise de connaissance, les faiblesses significatives de contrôle interne identifiées au niveau approprié au sein de l'entité.

(4) Cf. NI XV (page 17) Pour rappel, en ce qui concerne les contrôles de l'entité, le commissaire aux comptes évalue la conception et la mise en œuvre de ces contrôles pour l'audit lorsqu'il :
- a identifié un risque significatif, quand bien même il ne souhaiterait pas s'appuyer sur ces contrôles (cas obligatoire indépendamment de la stratégie d'audit) ;
- considère que les contrôles de substance seuls ne permettront pas d'obtenir les éléments suffisants et appropriés pour conclure sur la ou les assertions à vérifier. Dans ce cas, il testera également leur efficacité en réalisant des tests de procédures si la conception et la mise en œuvre des contrôles sont satisfaisantes (cas obligatoire indépendamment de la stratégie d'audit) ;
- souhaite s'appuyer sur les contrôles de l'entité pour réduire le risque d'anomalies significatives et/ou pour limiter l'étendue des contrôles de substance à mettre en œuvre.

(5) ITGC : Information Technology General Control.

Retrouvez les normes d'exercice professionnel et les notes d'information **sur SIDONI**

Fiche n°3

Les contrôles généraux informatiques ITGC

Retour Sommaire

***Préambule** : Pour s'assurer que les éléments de l'environnement informatique (applications, bases de données, …) fonctionnent comme attendu, l'entité met en place des processus de gestion des systèmes informatiques qui permettent de répondre aux risques que l'environnement informatique ne fonctionne pas comme prévu.*

Les contrôles généraux informatiques (ITGC) sont les contrôles mis en place par l'entité sur ces processus de gestion des systèmes informatiques pour s'assurer qu'ils atteignent leur objectif. Ils assurent que les contrôles liés au système informatique fonctionnent correctement tel que prévu, et tout au long de l'année.

(1) ITGC : Information Technology General Controls.

(2) ITAC : Information Technology Application Control.

(3) IPE : Information Produite par l'Entité.

I - Position dans la démarche d'audit

A l'issue de la compréhension des processus clés et des systèmes informatiques sous-jacents pertinents pour l'audit (cf. fiche n°2), le commissaire aux comptes a défini sa stratégie d'audit, laquelle peut prévoir de tester les contrôles généraux informatiques (ITGC)(1).

Lorsque le commissaire aux comptes décide de s'appuyer sur les contrôles généraux informatiques mis en place dans l'entité sur les applications supportant les contrôles automatisés ou manuels avec une composante informatique (ITAC)(2) ou les informations produites par l'entité (IPE)(3), il met en oeuvre les diligences prévues dans la présente fiche.

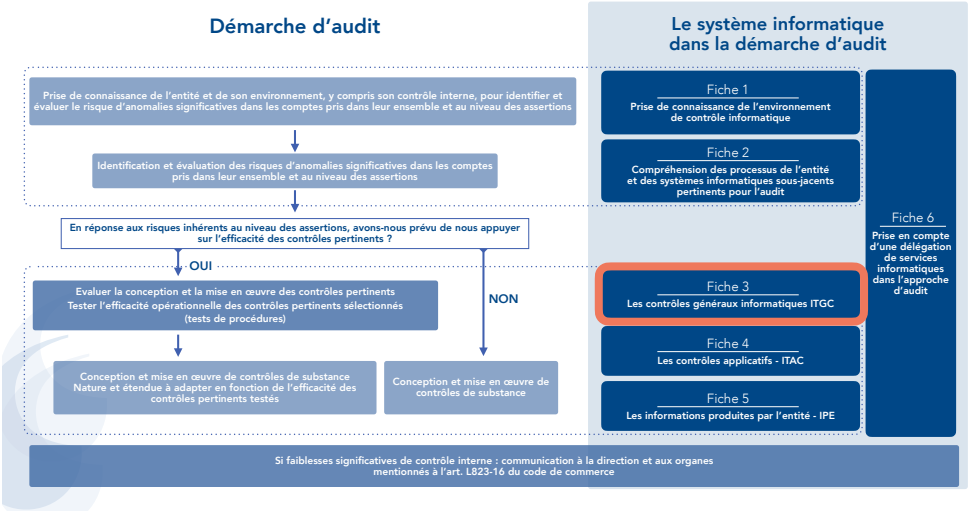
>>> voir schéma page suivante

FICHES AUDIT SI

Une **liste d'exemples de contrôles généraux informatiques** (ITGC) considérés en pratique comme généralement pertinents est proposée dans l'outil en annexe.

NEP 315
Prise de connaissance

NI XV
Approche par les risques



II - Objectifs

Les objectifs de cette fiche sont de permettre au commissaire aux comptes :

- ☑ D'identifier les risques liés aux processus de gestion des systèmes informatiques susceptibles de générer des anomalies significatives sur les comptes ;
- ☑ D'identifier les contrôles généraux informatiques (ITGC) pertinents répondant à ces risques ;
- ☑ D'évaluer la conception et la mise en œuvre de ces contrôles généraux informatiques (ITGC), ainsi que de tester, le cas échéant, leur efficacité opérationnelle ;
- ☑ D'analyser, le cas échéant, l'impact des faiblesses de contrôle interne relevées au sein des ITGC sur l'efficacité des contrôles applicatifs (ITAC) et sur l'intégrité des données des informations produites par l'entité (IPE), ainsi que les conséquences sur la stratégie d'audit en définissant les éventuelles procédures d'audit complémentaires à mettre en œuvre.

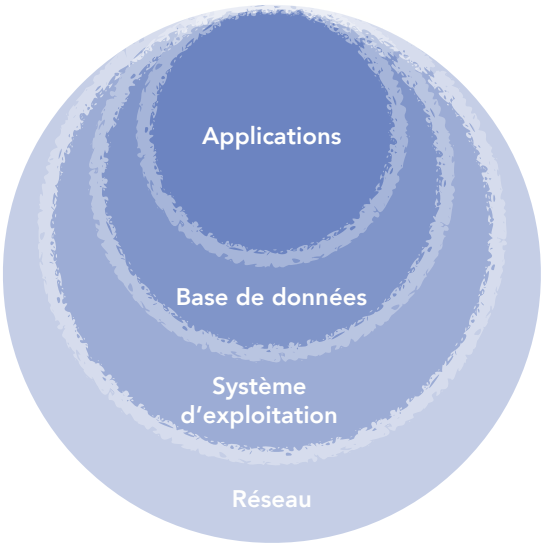
III - Diligences du commissaire aux comptes

1. Les risques au sein des processus de gestion du système informatique

Les différents types de processus de gestion du système informatique sont les suivants :

- gestion des accès,
- gestion des changements,
- gestion de l'exploitation informatique,
- gestion des projets informatiques, si pertinent.

Les risques au sein des processus de gestion du système informatique s'apprécient pour les différentes couches de l'environnement informatique en fonction de leurs technologies et au regard des contrôles automatisés, des contrôles manuels avec une composante informatique et des données des IPE sur lesquels le commissaire aux comptes souhaite s'appuyer. Les différentes couches de l'environnement informatique sont illustrées à l'aide du schéma suivant :



- **L'application** est le point d'entrée des utilisateurs métiers (direction financière, comptable, achats, …) pour saisir, modifier ou consulter les transactions ainsi que pour produire des IPE. La couche « application » comporte les risques les plus importants au regard de l'efficacité des contrôles applicatifs (ITAC) et de l'intégrité des données des IPE.
- **La base de données** organise et stocke les transactions ainsi que les données traitées par l'application. Cette couche comporte également des risques importants notamment quant à un accès direct à ces données ou à la modification de la structure de la base. Il peut s'agir de bases de données sous-jacentes à l'application ou d'un entrepôt de données (« *Datawarehouse* ») alimenté par l'application (par exemple pour le stockage des données des IPE).
- **Le système d'exploitation** sous-jacent à toute application permet à tous les composants matériels et logiciels de communiquer entre eux. Les risques liés au système d'exploitation relèvent donc du bon fonctionnement des applications. Un accès au système d'exploitation peut permettre un accès direct à la base de données.
- **Le réseau** est l'ensemble des équipements reliés entre eux permettant d'échanger des informations à l'intérieur ou à l'extérieur de l'entité. Des risques peuvent exister en cas de transmissions de données avec des tiers.

Les principaux risques résultant des différents types de processus de gestion des systèmes informatiques sont notamment les suivants :

- **Gestion des accès**
  - Les dispositifs d'identification et d'authentification (mot de passe) ne sont pas suffisamment robustes ;
  - Les créations et modifications des accès ne sont pas autorisées ;
  - Les droits d'accès des utilisateurs ne sont pas désactivés dans un délai raisonnable ;
  - Les droits d'accès ne sont pas appropriés au regard des responsabilités des utilisateurs ;
  - Les accès privilégiés (par exemples les comptes administrateur ou super utilisateur, …) ne sont pas suffisamment restreints ou supervisés ;
  - etc.

- **Gestion des changements**
  - Les changements sur les applications, les bases de données et le système d'exploitation ou les modifications de paramétrages ne sont pas autorisés, testés et validés par les personnes appropriées avant une mise en production ;
  - La séparation des fonctions entre les activités de développement et de mise en production ne permet pas de s'assurer que seuls les changements validés, sont mis en production.

- **Gestion de l'exploitation informatique**
  - Les incidents relatifs aux traitements informatiques ne sont pas identifiés ou résolus de manière appropriée ;
  - La gestion des outils de planification des traitements informatiques ou des interfaces (par exemple : ordonnanceurs, outils de gestion des flux, …) n'est pas en adéquation avec les besoins de l'entité ;
  - etc.

- **Gestion des projets informatiques**
  - Le pilotage du projet n'est pas approprié au regard des enjeux et de la complexité du projet ;
  - Les fonctionnalités, les interfaces et les droits d'accès ne sont pas suffisamment testés avant la mise en production ;
  - La stratégie et les contrôles relatifs à la migration des données ne garantissent pas une reprise exacte et exhaustive des données dans le nouveau système ;
  - etc.

2. Les contrôles généraux informatiques (ITGC) pertinents en réponse aux risques définis ci-dessus

Les contrôles généraux informatiques (ITGC) sont des contrôles sur les processus supportant le système d'informatique qui peuvent être réalisés sous la responsabilité de la DSI (direction du service informatique) et/ou d'autres services au sein de directions métiers, selon l'organisation de l'entité.

Le cas échéant, ces ITGC peuvent être exécutés en partie par des prestataires externes (dans ce cas, il convient de se référer à la fiche n° 6 - Prise en compte d'une délégation de services informatiques dans l'approche d'audit).

Ces contrôles généraux informatiques (ITGC) contribuent à la fiabilité et la stabilité des applications sur la période auditée. En conséquence, les ITGC concourent à l'efficacité des contrôles applicatifs (ITAC) et à l'intégrité des données des IPE (définis dans les fiches n°4 et n°5) sur lesquels le commissaire aux comptes a l'intention de s'appuyer dans le cadre de son audit.

En fonction des risques identifiés ci-dessus, en lien avec les contrôles automatisés, les contrôles manuels avec une composante informatique et les IPE, le commissaire aux comptes identifie les contrôles généraux informatiques (ITGC) pertinents répondant à ces risques.

> *Par exemple, lorsque le commissaire aux comptes souhaite s'appuyer sur un contrôle automatisé dans une application, il s'interroge sur les risques éventuels liés à la gestion des évolutions de cette application (ainsi que des bases de données et des systèmes d'exploitation sous-jacents si pertinents) et teste les ITGC pertinents couvrant ces risques.*

3. L'évaluation de la conception et de la mise en œuvre de ces contrôles généraux informatiques (ITGC), et les tests d'efficacité opérationnelle

3.1. Objectif, nature et étendue des tests d'ITGC

Selon l'approche d'audit retenue et sa connaissance de l'environnement de contrôle interne informatique, acquise à l'issue de la phase de prise de connaissance y compris des contrôles généraux informatiques (ITGC), le commissaire aux comptes peut :

- procéder à l'évaluation de la conception et de la mise en œuvre des ITGC, et le cas échéant, tester leur efficacité opérationnelle,
- ou à défaut, mettre en œuvre des procédures alternatives.

L'évaluation de la conception et de la mise en œuvre, ainsi que les tests d'efficacité opérationnelle sont similaires dans leur réalisation à la méthodologie appliquée par le commissaire aux comptes dans le cadre des contrôles métiers (il convient alors de se référer à la note d'information XV – Le commissaire aux comptes et l'approche d'audit par les risques – sections 4.13 B) et 4.22).

Les tests d'efficacité opérationnelle, appelés tests de procédures dans les normes d'exercice professionnel, ont pour but de vérifier que les contrôles de l'entité sont réalisés :

- selon les modalités prévues ;
- aux moments adéquats ;
- de façon constante tout au long de la période contrôlée ;
- par la bonne personne ou le bon moyen.

Lorsque le commissaire aux comptes met en œuvre des tests de procédure, il peut apparaître nécessaire d'apprécier la fiabilité des éléments sous-tendant le contrôle (comme une information produite par l'entité – IPE).

> *Par exemple, le contrôle peut consister à revoir un état, telle que la revue de la liste des utilisateurs, il est alors nécessaire dans le test de procédure d'inclure une étape visant à apprécier la fiabilité (exhaustivité et exactitude) de l'état lui-même (cf. fiche n°5 Les informations produites par l'entité – IPE).*

3.2. Calendrier des tests des contrôles généraux informatiques (ITGC)

Le commissaire aux comptes doit s'assurer que les contrôles généraux informatiques (ITGC) fonctionnent sur l'ensemble de la période auditée. Il planifie son intervention en une ou plusieurs étapes.

En termes de calendrier, les tests des ITGC sont généralement réalisés avant la clôture des comptes.

En pratique, la période couverte par les tests des ITGC pourrait être de 9 mois sur l'exercice audité. Dans ce cas, pour la période restant à couvrir jusqu'à la fin de l'exercice (cf. paragraphe 13 de la NEP 330), le commissaire aux comptes détermine les éléments complémentaires à collecter. Par exemple, il peut s'assurer a minima par entretien que le contrôle n'a pas évolué dans sa conception et sa mise en œuvre.

Si des changements sont intervenus pendant la période non couverte par les tests des ITGC (par exemple : changement de responsable de contrôle, mise à jour de la conception du contrôle…), des procédures additionnelles peuvent être nécessaires pour évaluer l'efficacité des ITGC sur l'ensemble de l'exercice (par exemple : retester l'ITGC impacté par cette évolution sur la période résiduelle).

IV - Incidences sur la démarche d'audit

Lorsque les tests des contrôles généraux informatiques (ITGC) ne font pas apparaître de faiblesses, cela implique que les applications fonctionnent comme prévu tout au long de la période. Cette conclusion est prise en compte dans les tests réalisés sur les contrôles applicatifs (ITAC) (cf. fiche 4) et sur l'intégrité des données des informations produites par l'entité (cf. fiche 5) qui dépendent de cette application.

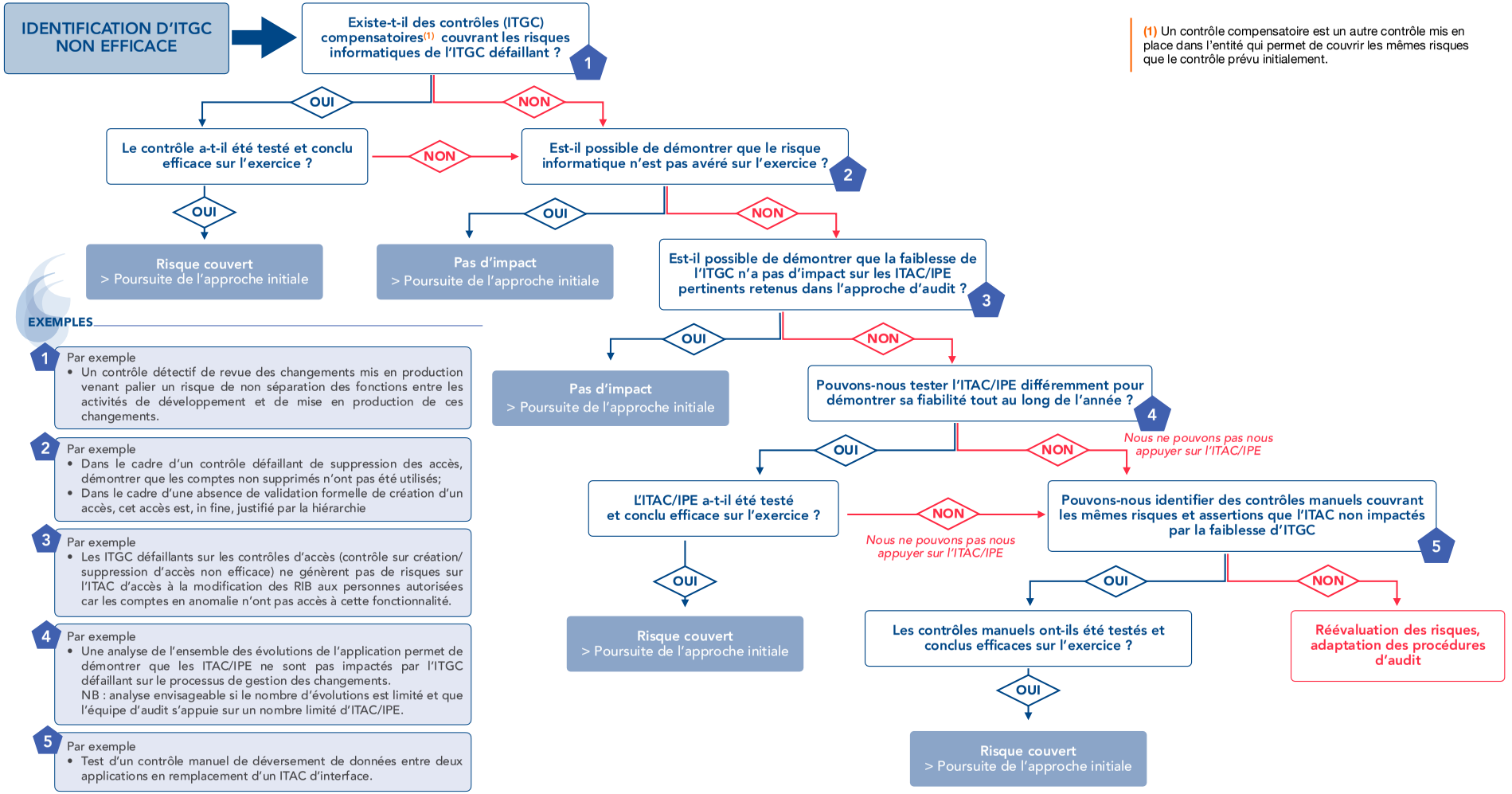
Lorsqu'il apparaît que la conception ou la mise en œuvre des ITGC n'est pas appropriée, ou que lors de la mise en œuvre des tests de procédures, les ITGC n'ont pas fonctionné comme prévu, le commissaire aux comptes procède à des analyses afin d'en comprendre les causes et d'en mesurer les conséquences sur l'efficacité des ITAC et sur l'intégrité des données des IPE et sur sa capacité à s'appuyer sur ces ITAC et ces IPE dans son approche d'audit. Il apprécie également si ces faiblesses impliquent l'identification de nouveaux risques ou un niveau de risque plus élevé qu'évalué initialement et met en œuvre des procédures pour y répondre.

> *Par exemple, l'absence de contrôles des opérations réalisées par les utilisateurs disposant de droits étendus peut amener le commissaire aux comptes à tester certaines de ces opérations pour confirmer leur caractère approprié.*

Les faiblesses ainsi identifiées lors de la prise de connaissance des processus de gestion des systèmes informatiques, et lors de la réalisation des tests sur les contrôles généraux informatiques (ITGC) font l'objet d'une communication au niveau approprié au sein de l'entité et au moment opportun.

En pratique, le commissaire aux comptes peut utilement s'appuyer sur l'arbre de décision (présenté à la page suivante) afin d'appréhender les différentes étapes à mettre en œuvre lorsque des faiblesses sont identifiées sur les ITGC.

FICHE AUDIT SI



(1) Un contrôle compensatoire est un autre contrôle mis en place dans l'entité qui permet de couvrir les mêmes risques que le contrôle prévu initialement.

EXEMPLES

1 Par exemple
- Un contrôle détectif de revue des changements mis en production venant palier un risque de non séparation des fonctions entre les activités de développement et de mise en production de ces changements.

2 Par exemple
- Dans le cadre d'un contrôle défaillant de suppression des accès, démontrer que les comptes non supprimés n'ont pas été utilisés;
- Dans le cadre d'une absence de validation formelle de création d'un accès, cet accès est, in fine, justifié par la hiérarchie

3 Par exemple
- Les ITGC défaillants sur les contrôles d'accès (contrôle sur création/ suppression d'accès non efficace) ne génèrent pas de risques sur l'ITAC d'accès à la modification des RIB aux personnes autorisées car les comptes en anomalie n'ont pas accès à cette fonctionnalité.

4 Par exemple
- Une analyse de l'ensemble des évolutions de l'application permet de démontrer que les ITAC/IPE ne sont pas impactés par l'ITGC défaillant sur le processus de gestion des changements.
  NB : analyse envisageable si le nombre d'évolutions est limité et que l'équipe d'audit s'appuie sur un nombre limité d'ITAC/IPE.

5 Par exemple
- Test d'un contrôle manuel de déversement de données entre deux applications en remplacement d'un ITAC d'interface.

Fiche n°4

Les contrôles applicatifs - ITAC

Retour Sommaire

I - Position dans la démarche d'audit

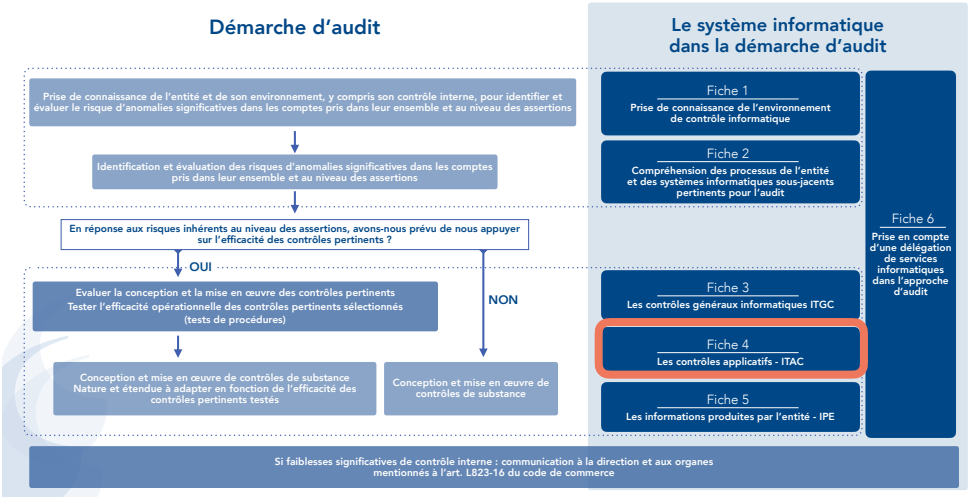
La fiche n°2 « Compréhension des processus clés et des systèmes informatiques sous-jacents pertinents pour l'audit » a permis d'identifier les contrôles applicatifs - ITAC(1) - (contrôles automatisés, et contrôles manuels avec une composante informatique) sur lesquels le commissaire aux comptes a l'intention de s'appuyer dans le cadre de son audit.

Les tests des contrôles généraux informatiques (ITGC(2)), permettant de s'assurer de l'efficacité de ces contrôles applicatifs (ITAC) tout au long de la période auditée, sont décrits dans la fiche n°3 « Les contrôles généraux informatiques – ITCG ».

Toutefois, dans le cas où le commissaire aux comptes décide de ne pas tester les contrôles généraux informatiques (ITGC), ou si les ITGC ne sont pas assez robustes, le commissaire aux comptes met en place des procédures alternatives afin de vérifier la stabilité des contrôles applicatifs (ITAC) tout au long de l'exercice.

(1) ITAC : Information Technology Application Control.

(2) ITGC : Information Technology General Controls.



Un exemple de papier de travail est proposé en annexe de cette fiche permettant de documenter l'évaluation des contrôles applicatifs par le commissaire aux comptes.

NEP 315
Prise de connaissance

NI XV
Approche par les risques

II - Objectifs

Les objectifs de cette fiche sont de permettre au commissaire aux comptes :

- ☑ D'apprécier la conception et la mise en œuvre des contrôles portés par les applications informatiques (les contrôles applicatifs – « ITAC ») pertinents pour l'audit au sens du §16 de la NEP 315 (cf. références normatives à la fin de la présente fiche) ;
- ☑ D'évaluer l'efficacité opérationnelle de ces contrôles sur toute la période ;
- ☑ D'analyser, le cas échéant, l'impact des ITAC défaillants sur la démarche d'audit retenue, notamment l'évaluation de contrôles compensatoires[3] et/ou la nature et l'étendue des contrôles de substance.

(3) Un contrôle compensatoire est un contrôle mis en place dans l'entité qui permet de couvrir les mêmes risques que le contrôle prévu initialement.

III - Diligences du commissaire aux comptes

Lors de la prise de connaissance des processus clés, le commissaire aux comptes a identifié des contrôles de l'entité pertinents pour l'audit[4] dont certains sont automatisés ou manuels avec une composante informatique (ITAC).

(4) Cf. NI XV Le commissaire aux comptes et l'approche d'audit par les risques (page 31) sur les aspects relatifs « aux contrôles de l'entité pertinents pour l'audit ».

1. Typologie des ITAC

Les ITAC incluent des contrôles automatisés ou des contrôles mixtes (c'est-à-dire intégrant une composante automatisée et une composante manuelle).

Différents types d'ITAC peuvent être identifiés dans le système d'information :

- Les contrôles automatisés portés par le système informatique qui peuvent être codés dans des programmes informatiques (de manière inhérente pour un progiciel du marché ou dans les programmes développés spécifiquement) ou configurés dans le paramétrage ;
  Par exemple : le paramétrage du contrôle de rapprochement commande / réception / facture pour le processus Achats (communément appelé le « 3 way match ») ; la validation par le système des données à la saisie ; l'existence de champs obligatoires à la saisie, ...
- Les contrôles d'accès et de séparation des tâches répondant directement à des risques dans les processus clés ;
  Par exemple : le profil d accès restreint pour la modification des prix de vente ; la revue périodique du respect de la séparation des tâches sur des risques métier ciblés ; le workflow de validation sur des validations de contrats, ...
- Des programmes de calculs spécifiques ;
  Par exemple : les calculs d'intérêts ou de provisions complexes, ...
- Des contrôles d'interface entre applications ;
  Les contrôles d'interface intègrent plusieurs dimensions : des contrôles automatisés permettant d'assurer l'exhaustivité et l'exactitude des flux transmis, ainsi qu'un état d'identification des anomalies/rejets.
  Par exemple : les contrôles liés à l'interface des flux de ventes journaliers dans le logiciel de comptabilité.

Bien que le commissaire aux comptes évalue toutes les composantes de nature automatisée ou manuelle ou s'appuyant sur une IPE, les sections ci-après de la fiche 4 ne traitent que de l'évaluation des composantes automatisées.

2. Evaluation de la conception et de la mise en œuvre des contrôles applicatifs - ITAC

L'objectif de cette étape est d'évaluer la pertinence du contrôle automatisé par rapport au risque identifié sur les assertions. Cette évaluation nécessite de prendre connaissance des règles de gestion supportant ce contrôle et de vérifier qu'elles permettent de répondre aux risques.

En particulier, le commissaire aux comptes s'interroge sur les aspects suivants :

- Les règles de gestion (ou « business rules » ou règles de paramétrage) et les critères de déclenchement du contrôle (seuils de tolérance/d'approbation, champs obligatoires, cohérence de données par rapport à un référentiel, …) ;
- Le périmètre des entités/sites concernés, et des transactions couvertes par le contrôle ;
- Les règles de calcul ;
- La fréquence du contrôle le cas échéant ;
- etc.

L'évaluation de la conception peut être réalisée de plusieurs façons mais ne peut pas se réduire à un simple entretien avec l'entité. En pratique, cela se traduit par l'inspection de documents également.

Lorsque le commissaire aux comptes conclut que la conception du contrôle est satisfaisante, il évalue si ce contrôle est correctement mis en œuvre. Il n'y a pas d'intérêt à évaluer la mise en œuvre du contrôle si sa conception n'est pas satisfaisante.

Dans le cadre de la mise en œuvre de ce contrôle, le commissaire aux comptes vérifie que celui-ci a été appliqué :

- sur la période auditée, et
- conformément aux règles de gestion prévues lors de sa conception.

Par exemple, le commissaire aux comptes sélectionne une transaction correspondant à chaque règle de gestion pertinente et s'assure du correct fonctionnement de l'application par observation. Le commissaire aux comptes peut, le cas échéant, faire une inspection du paramétrage (notamment en présence d'un progiciel du marché).

En fonction de la complexité technique du test à mettre en œuvre, le commissaire aux comptes utilisera les travaux d'un auditeur spécialisé dans les systèmes informatiques.

3. Tests d'efficacité opérationnelle des contrôles applicatifs - ITAC

Pour les contrôles applicatifs (ITAC) sur lesquels le commissaire aux comptes a l'intention de s'appuyer, il s'assure que ces ITAC fonctionnent comme prévu tout au long de l'exercice. Il convient alors de couvrir les risques informatiques impactant l'efficacité opérationnelle de ces ITAC tout au long de la période auditée.

Ces risques sont, en général, couverts par les contrôles généraux informatiques (ITGC) sur les applications supportant les contrôles automatisés ou manuels avec une composante informatique, que le commissaire aux comptes a testés (cf. fiche n°3 – Les contrôles généraux informatiques - ITGC).

Dans ce cas, l'évaluation de la mise en oeuvre de l'ITAC (réalisée à l'étape précédente) couplée à des tests sur les ITGC jugés satisfaisants permettent de s'assurer de la fiabilité et de la stabilité de l'ITAC sur toute la période auditée. Le commissaire aux comptes n'a donc pas à mettre en œuvre de tests de procédures sur cet ITAC.

Toutefois, pour certains ITAC, le commissaire aux comptes peut être amené à réaliser, en plus, des procédures permettant de couvrir des risques spécifiques.

Par exemple :

- *Pour un contrôle automatisé configuré dans le paramétrage de l'application :*
  - *la restriction des accès aux personnes autorisées à la modification du paramétrage et robustesse de l'authentification à l'application,*
  - *le processus de mise à jour du paramétrage (demande, test, validation).*
- *Pour un contrôle d'interface :*
  - *la supervision des flux d'interface, l'identification et la correction des anomalies et rejets,*
  - *le processus de gestion des évolutions des applications concernées par l'interface,*
  - *la restriction des accès aux personnes autorisées à la modification de l'interface et robustesse de l'authentification à l'application,*
  - *en cas d'utilisation d'outils de type « ordonnanceur » ou les outils intermédiaires de gestion de flux :*
    - *le processus de gestion des évolutions de ces outils,*
    - *la restriction des accès aux personnes autorisées à la modification de ces outils et robustesse de l'authentification à ces outils.*

Si le commissaire aux comptes n'est pas en mesure de s'appuyer sur les contrôles généraux informatiques - ITGC (cf. arbre de décision de la fiche n°3), il met en œuvre des procédures alternatives[5] pour conclure sur l'efficacité opérationnelle des ITAC sur l'ensemble de l'exercice. Par exemple, sur le processus de gestion des changements, si les ITGC sont défaillants, le commissaire aux comptes met en œuvre une procédure alternative consistant à analyser les évolutions susceptibles d'impacter l'ITAC.

(5) Une procédure alternative est réalisée par le commissaire aux comptes afin de lui permettre de collecter les éléments qu'il estime nécessaires pour vérifier les assertions faisant l'objet du contrôle initialement prévu.

L'approche à privilégier reste toutefois le test des contrôles généraux informatiques - ITGC (qui inclut le cas échéant l'analyse d'impact des faiblesses des ITGC pour couvrir les risques informatiques), car ils contribuent à un environnement de contrôle robuste.

IV – Incidences sur la démarche d'audit

A l'issue des tests réalisés sur les contrôles applicatifs - ITAC, le commissaire aux comptes évalue les conséquences sur sa démarche d'audit.

Lorsqu'il apparaît que les contrôles n'ont pas fonctionné comme prévu, le commissaire aux comptes apprécie notamment la nécessité de répondre aux risques d'anomalies significatives par la mise en œuvre de contrôles de substance plus étendus.

Si des faiblesses significatives sont identifiées, il communique ces faiblesses par écrit à la direction de l'entité et aux organes de gouvernance, conformément à la NEP 265. S'agissant des autres faiblesses, le commissaire aux comptes apprécie, en fonction de son jugement professionnel, l'opportunité de les communiquer au niveau approprié au sein de l'entité.

Références normatives

V.I. NEP 315
Connaissance de l'entité et de son environnement et évaluation du risque d'anomalies significatives

16. Le commissaire aux comptes évalue la conception et la mise en œuvre des contrôles de l'entité lorsqu'il estime :

- qu'ils contribuent à prévenir le risque d'anomalies significatives dans les comptes, pris dans leur ensemble ou au niveau des assertions ;
- qu'ils se rapportent à un risque inhérent élevé identifié qui requiert une démarche d'audit particulière. Un tel risque est généralement lié à des opérations non courantes en raison de leur importance et de leur nature ou à des éléments sujets à interprétation, tels que les estimations comptables ;
- que les seuls éléments collectés à partir des contrôles de substance ne lui permettront pas de réduire le risque d'audit à un niveau suffisamment faible pour obtenir l'assurance recherchée.

Retrouvez les normes d'exercice professionnel et les notes d'information **sur SIDONI**

Le système informatique dans la démarche d'Audit

Fiche n°5

Les informations produites par l'entité - IPE

Retour Sommaire

Préambule *: Les IPE représentent toutes les informations produites par l'entité que le commissaire aux comptes utilise dans le cadre de ses procédures d'audit qu'elles soient produites par des applications informatiques, des outils tels que Word ou Excel (appelés plus généralement "outils bureautiques"), ou par tout autre moyen, y compris manuellement. A noter que les différents états comptables constituant la comptabilité ne sont pas en eux- mêmes des informations produites par l'entité (journaux, grands-livres, balance générale, balances auxiliaires, …).*(1)

(1) Cf. chronique CNP 2020-07 – Informations produites par l'entité.

I - Position dans la démarche d'audit

(2) ITAC : Information Technology Application Control.

Les normes d'exercice professionnel (NEP) ne définissent pas la notion d'« information produite par l'entité ». Néanmoins, le paragraphe 6 de la NEP 500 traite du caractère suffisant et approprié (probant) des éléments collectés et a pour objet d'affirmer que les éléments collectés d'origine externe sont plus fiables que ceux d'origine interne (les informations produites par l'entité faisant partie des « éléments collectés d'origine interne »).

La fiche n°2 « Compréhension des processus clés et des systèmes informatiques sous-jacents pertinents pour l'audit » a permis d'identifier les contrôles applicatifs – ITAC(2) (détaillés dans la fiche n°4) et également les informations produites par l'entité (IPE) sur lesquels le commissaire aux comptes a l'intention de s'appuyer dans le cadre de son audit.

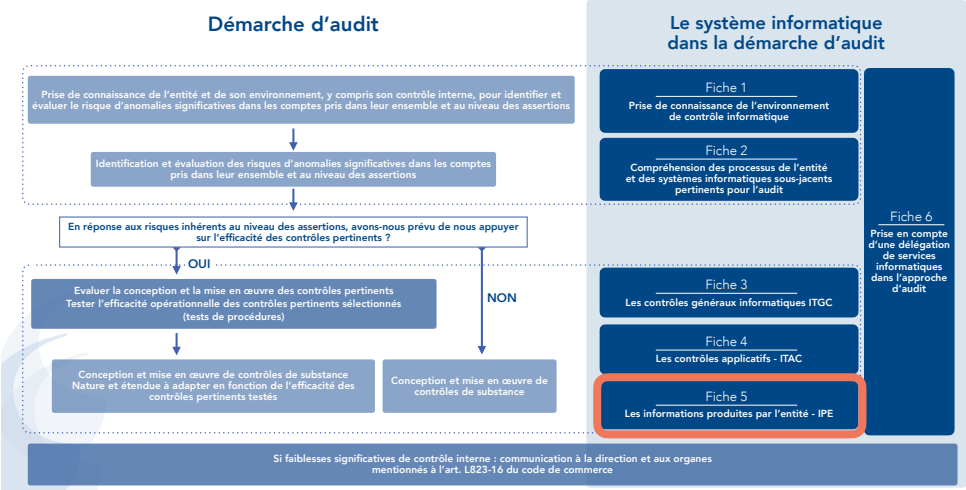
Lorsque le commissaire aux comptes s'appuie sur des informations produites par l'entité (IPE), il collecte des éléments probants sur le caractère fiable (exhaustivité et exactitude) et pertinent de ces IPE.

Pour ce faire, il apprécie si les données de l'IPE :

- sont suffisamment précises et détaillées (i.e. le « caractère pertinent »),
- sont exactes et exhaustives (i.e. le « caractère fiable »).

Les contrôles généraux informatiques (ITGC), décrits dans la fiche n°3, concourent à l'intégrité des données des IPE.

>>> voir schéma page suivante



Un exemple de papier de travail est proposé en annexe de cette fiche permettant de documenter l'appréciation de la fiabilité de l'IPE par le commissaire aux comptes.

II - Objectifs

L'objectif de cette fiche est d'apporter des précisions sur la notion de fiabilité des informations produites par l'entité (IPE) sur lesquelles le commissaire aux comptes a l'intention de s'appuyer pour la réalisation de certaines procédures d'audit.

Ce caractère fiable peut s'apprécier, en fonction des circonstances :

- Par des tests de procédures sur les contrôles de l'entité relatifs à l'IPE ;
- Par des sondages sur un certain nombre d'éléments inclus dans cette IPE.

Cette fiche n'aborde pas les contrôles effectués par méthode de sondage.

III - Diligences du commissaire aux comptes

1. Identification des informations produites par l'entité (IPE) selon leur utilisation dans l'approche d'audit

Le commissaire aux comptes identifie les informations produites par l'entité (IPE) sur lesquelles il va s'appuyer lors de la réalisation de ses procédures d'audit définies en réponse au risque d'anomalies significatives dans les comptes.

Exemples d'IPE utilisées par l'entité dans son contrôle interne :

- *Le rapport d'anomalies utilisé par l'entité lors de l'analyse des factures bloquées au paiement,*
- *Le rapport d'anomalies listant les rejets d'interface utilisé par l'entité,*

NEP 315 Prise de connaissance

NI XV Approche par les risques

- *L'extraction des comptes utilisateurs utilisés par l'entité dans sa revue périodique des accès (ITGC),*
- *La liste des modifications de RIB utilisées par l'entité dans son contrôle détectif sur le caractère approprié de ces modifications.*

Exemples d'IPE utilisées par le commissaire aux comptes dans les tests de procédures :

- *La liste des changements sur la période utilisée pour le test d'efficacité sur les ITGC,*
- *La liste des nouveaux employés créés dans l'application dédiée pour le test d'efficacité du contrôle de l'entité sur la création des dossiers des employés.*

Exemples d'IPE utilisées lors des contrôles de substance :

- *La balance âgée pour l'analyse des dépréciations des créances clients,*
- *Le fichier Excel de calcul d'une provision,*
- *Le listing des stocks utilisé pour l'inventaire physique,*
- *La liste des litiges,*
- *L'extraction des mouvements de sorties de stocks pour les rapprocher de la facturation.*

Il est important de préciser que seules les IPE utilisées dans l'approche d'audit sont à considérer comme pertinentes pour l'audit.
Certaines de ces IPE peuvent comprendre de nombreuses données, dont des données pas nécessairement utiles dans le cadre des procédures d'audit définies par le commissaire aux comptes. Il convient alors que ce dernier identifie les données qui sont pertinentes pour ses travaux.

A noter que des IPE peuvent être produites dans le cadre des délégations de service et peuvent, le cas échéant, être utilisées par le commissaire aux comptes si elles sont considérées comme pertinentes.

2. Prise de connaissance et identification des risques à couvrir

Lorsque le commissaire aux comptes identifie des IPE sur lesquelles il s'appuie lors de la réalisation de ses procédures d'audit, la prise de connaissance du flux d'informations depuis l'entrée des données dans le système d'information jusqu'à la génération de l'IPE, lui permet d'apprécier quels éléments collecter.

En fonction des circonstances, les risques que le commissaire aux comptes cherche à couvrir peuvent être :

- Des risques liés à l'entrée des données de l'IPE (i.e. le risque que les données ne soient pas correctement / exhaustivement entrées dans le SI de l'entité),

Par exemple, les données relatives aux expéditions sont saisies manuellement et une erreur ou un oubli de saisie peut se produire.

- Des risques liés à l'intégrité des données qui seront utilisées pour l'IPE, notamment :
  - les données sont altérées durant les traitements ou lors de leur stockage dans le système,
  - les données ne sont pas correctement transférées d'un élément du SI de l'entité à l'autre (application, *datawarehouse* (entrepôt de données), …).
- Des risques liés à la génération de l'IPE :
  - le programme ou la requête de génération de l'IPE ne permet pas d'extraire des données pertinentes et exhaustives,

    Par exemple, le programme proposant les produits à compter quotidiennement dans le cadre d'une procédure d'inventaire tournant omet une catégorie de produits .
  - les paramètres saisis pour générer l'IPE ne sont pas corrects,

    Par exemple, la requête souhaitée est sur le mois de mars mais l'utilisateur a saisi « avril ».
  - les calculs ou traitements (par exemple, les tris) effectués par le programme générant l'IPE sont inexacts ou erronés,

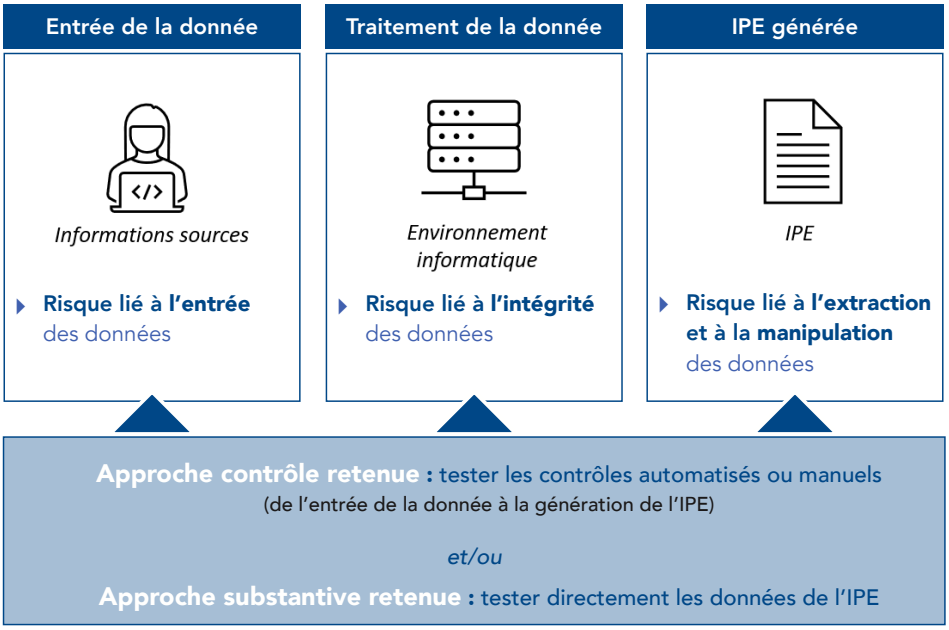
    Par exemple, dans une balance âgée clients, le calcul de la date d'échéance et la présentation des factures dans la tranche d'échéance inappropriée.
- Des risques liés à la manipulation des données de l'IPE :
  - une fois extraites, les données de l'IPE peuvent avoir été modifiées ou supprimées,
  - les données extraites n'ont pas été correctement retraitées ou présentées du fait d'utilisation de filtres, tris, calculs…,

    Par exemple, le contrôleur de gestion extrait dans Excel le listing des stocks à rotation lente, puis ajoute manuellement les colonnes nécessaires au calcul de la provision pour dépréciation, des erreurs sont possibles dans ces opérations manuelles complémentaires.

Tous les risques ne sont pas systématiquement pertinents. Le commissaire aux comptes apprécie, selon son jugement professionnel, les risques au regard du contexte, de la nature et du système d'information de chaque IPE.

Par exemple, lorsque l'entité suit certains contrats importants pluriannuels directement sous Excel, le risque lié à la génération de l'IPE ne sera pas applicable.

La démarche d'audit à retenir et l'identification des risques à couvrir sont schématisés ci-dessous :



3. Procédures d'audit mises en œuvre pour répondre aux risques identifiés

Le commissaire aux comptes exerce son jugement professionnel pour déterminer la nature, l'étendue et le calendrier des procédures d'audit à mettre en œuvre pour collecter les éléments probants relatifs à la fiabilité des IPE, en fonction des risques identifiés.

Les procédures d'audit peuvent être de deux types :

- **Des tests de procédures.**
  Pour couvrir les risques, le commissaire aux comptes choisit de tester l'efficacité opérationnelle de contrôles mis en œuvre par l'entité visant à fiabiliser les IPE.
- **Des contrôles de substance sur des éléments composant l'IPE**
  Lorsque le commissaire aux comptes choisit de ne pas s'appuyer sur l'efficacité opérationnelle des contrôles relatifs à l'IPE, il collecte les éléments probants relatifs au caractère fiable des IPE par le biais de procédures de rapprochement avec la comptabilité et/ou en corroborant avec une autre source par sondages sur un certain nombre d'éléments.

Pour définir l'étendue des travaux visant à collecter des éléments probants sur l'IPE, le commissaire aux comptes exerce son jugement professionnel et peut prendre en compte notamment :

- L'utilisation de l'IPE dans l'approche d'audit (par exemple, les travaux sur les IPE obtenues lors de la phase de planification de la mission seront moins étendus que ceux réalisés sur les IPE utilisées dans le cadre de tests de procédures ou de contrôles de substance) ;
- Le niveau de risque d'anomalies significatives sur les comptes concernés ;

- La complexité de l'IPE et ;
- Les autres procédures d'audit ayant déjà permis de collecter des éléments concourant à la fiabilité de l'IPE.

A noter que sur une même IPE, le commissaire aux comptes peut mettre en œuvre un test de procédure sur un risque identifié de l'IPE (par exemple sur le programme de génération de l'IPE) et un contrôle de substance sur un autre risque (par exemple sur l'exhaustivité et l'exactitude des données entrées).

Dans certaines circonstances, les contrôles de substance mis en œuvre, par ailleurs, par le commissaire aux comptes permettent d'obtenir directement des éléments probants sur l'IPE. Deux cas de figures sont alors possibles :

- Les preuves d'audit corroborent des informations présentes sur l'IPE (ex : sur les nombres de jours de congés payés par personne lors des contrôles de substance sur la provision pour congés payés). Dans ce cas, les contrôles de substance permettent également d'obtenir des éléments probants sur la fiabilité de l'IPE.
- Les preuves d'audit obtenues ne portent pas spécifiquement sur les informations présentes sur l'IPE (ex : prévision des volumes de vente justifiant une dépréciation de stocks). Dans ce cas, des travaux complémentaires seront nécessaires sur la fiabilité de l'IPE.

Les procédures d'audit pour collecter les éléments probants sur une IPE sont à mettre en œuvre à chaque utilisation de cette IPE.

IV - Incidences sur la démarche d'audit

Lorsque le commissaire aux comptes a obtenu les éléments probants suffisants et appropriés sur la fiabilité de l'IPE, il peut s'appuyer sur cette IPE dans le cadre de ses travaux.

En revanche, si le commissaire aux comptes identifie des anomalies, il analyse la nature de ces anomalies et les conséquences sur la procédure d'audit supportée par l'IPE, selon son jugement professionnel. Il en tire les conséquences sur la nature et l'étendue des procédures d'audit à mettre en œuvre, le cas échéant.

- Dans le cas où l'IPE est utilisée par l'entité dans le cadre de son contrôle interne, il convient d'évaluer si les anomalies décelées sur les IPE remettent en cause l'évaluation du contrôle dans sa conception, sa mise en œuvre et son efficacité opérationnelle.
- Dans le cas où l'IPE est utilisée par le commissaire aux comptes dans ses contrôles de substance, il met en œuvre, le cas échéant, des procédures alternatives(3).

(3) Une procédure alternative est réalisée par le commissaire aux comptes afin de lui permettre de collecter les éléments qu'il estime nécessaires pour vérifier les assertions faisant l'objet du contrôle initialement prévu.

Les anomalies identifiées lors des diligences mises en œuvre sur les IPE, peuvent faire l'objet d'une communication au niveau approprié au sein de l'entité en application des NEP 260 - Communications avec les organes mentionnés à l'article L. 823-16 du code de commerce et NEP-265- Communication des faiblesses du contrôle interne.

Fiche n°6

Prise en compte d'une délégation de services informatiques dans l'approche d'audit

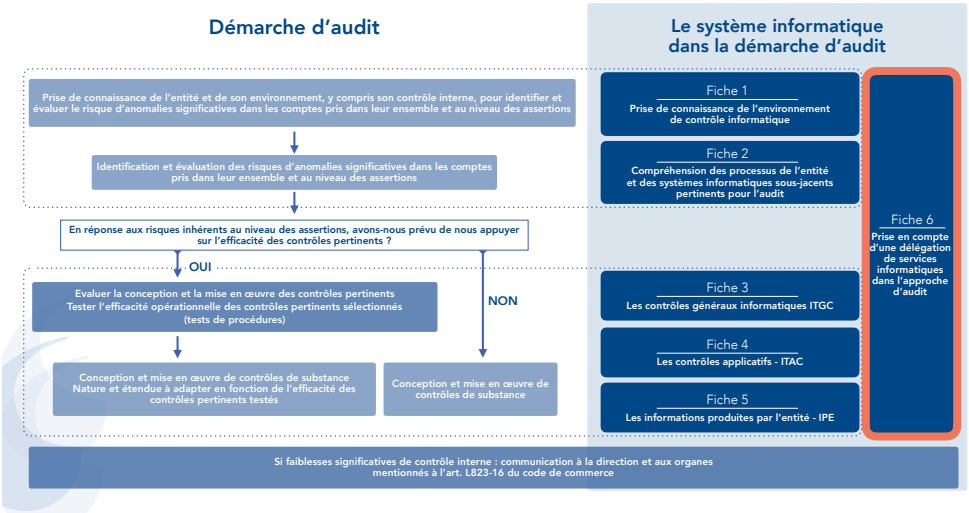
Retour Sommaire

Préambule *: Cette fiche porte sur les délégations de services informatiques et ne traite donc pas de tous les cas de délégations de services pouvant exister dans l'entité auditée (par exemple, pour la gestion de la paie). Pour les cas particuliers de centres de services partagés, se référer à la Note d'information XIX - Le commissaire aux comptes et l'audit d'une entité ayant recours aux services d'un centre de services partagés au sein d'un groupe.*

(1) Lorsque le commissaire aux comptes collecte le rapport d'assurance uniquement pour documenter sa prise de connaissance des processus sous-traités au prestataire, il formalise ces travaux directement dans le cadre des fiches n°1 et 2.

I - Position dans la démarche d'audit

Cette fiche n°6 « Prise en compte d'une délégation de services informatiques dans l'approche d'audit » vient compléter les fiches n°1 à n°5 lorsqu'il existe une délégation de services.



Un exemple de papier de travail est proposé en annexe de cette fiche formalisant l'appréciation du commissaire aux comptes sur le rapport d'assurance relatif au dispositif de contrôle interne mis en œuvre par un prestataire dans le cadre d'une délégation de service(1).

II - Objectifs

Cette fiche a pour objectifs de permettre au commissaire aux comptes de :

- ☑ Comprendre la nature et l'étendue de la délégation de services,
- ☑ Définir la démarche d'audit à retenir lorsque l'entité auditée fait appel à une délégation de services,
- ☑ Préciser les procédures à mettre en œuvre lorsqu'il s'appuie sur un rapport d'assurance relatif au dispositif de contrôle interne du prestataire.

Cette approche est à décliner uniquement sur les applications, y compris leurs infrastructures sous-jacentes, considérées comme pertinentes à l'issue de la compréhension des processus clés (cf. fiche n°2).

III - Diligences du commissaire aux comptes

Dans le cadre de sa prise de connaissance du SI (cf. fiche n°1 – Prise de connaissance de l'environnement de contrôle informatique), le commissaire aux comptes identifie les systèmes et les activités informatiques qui font l'objet d'une délégation de services.

Il prend notamment en compte les éléments suivants :

- La nature des services fournis par le prestataire et leur importance pour l'entité utilisatrice, y compris leur incidence sur le contrôle interne de l'entité auditée,
- La nature et le caractère significatif des opérations traitées par le prestataire de services ou des comptes ou processus d'informations financières affectés par les prestations qu'il fournit,
- Le degré d'interaction entre les activités du prestataire et celles de l'entité utilisatrice,
- La nature de la relation entre l'entité utilisatrice et le prestataire, y compris les conditions contractuelles pertinentes pour les prestations fournies.

Pour ce faire, il pourra se référer au contrat de services signé avec le prestataire, aux processus et contrôles mis en place en interne chez l'entité auditée pour suivre la bonne exécution de la prestation (par exemple, indicateurs clés définis dans le contrat de niveau de service (« *Service Level Agreement* »)).

Les services fournis peuvent être les suivants :

- Hébergement des infrastructures informatiques chez un prestataire (par exemple mise à disposition d'un *Data Center* et/ou une infrastructure en mode Cloud public / privé / hybride),
- Infogérance (exploitation) des infrastructures informatiques par un prestataire,
- Utilisation d'une plateforme et d'outils de développement fournis par un prestataire (PaaS – *Platform as a Service*),

NEP 315 Prise de connaissance

NI XV Approche par les risques

- Maintenance des applications par un prestataire (qui peut être ou non l'éditeur de l'application),
- Utilisation d'une application hébergée et maintenue par un prestataire (cas des applications en mode *SaaS – Software as a Service*).

Il convient d'identifier également les cas où le prestataire confie certaines de ces activités entrant dans le champ de l'audit à un ou plusieurs autres prestataires.

Au regard du contrôle interne, le commissaire aux comptes prend connaissance de la répartition des rôles sur la mise en œuvre des contrôles et leur supervision entre l'entité auditée et le prestataire.

Dès lors que le commissaire aux comptes s'appuie sur les contrôles généraux informatiques (ITGC[2]) :

- pour les contrôles pertinents pour l'audit dont l'entité assure la mise en œuvre ou la supervision, le commissaire aux comptes met en œuvre la démarche décrite dans la fiche n°3,
- pour les contrôles pertinents pour l'audit dont l'entité n'assure pas la mise en œuvre ou la supervision, le commissaire aux comptes obtient des éléments probants qui lui permettent d'aboutir à des conclusions à partir desquelles il fonde son opinion sur les comptes[3].

Deux situations peuvent alors exister :

❖ **Cas 1 :** Le commissaire aux comptes peut s'appuyer sur un rapport d'assurance[4] fourni par l'entité auditée[5] portant sur le dispositif de contrôle interne mis en œuvre par le prestataire de services. Il existe deux types de rapport d'assurance :

- Un rapport de type I sur la description et la conception des contrôles mis en œuvre par le prestataire de services ;
- Un rapport de type II sur la description, la conception et l'efficacité des contrôles mis en œuvre par le prestataire de services, nécessaire pour pouvoir s'appuyer sur l'efficacité des ITGC.

- **Points d'attention :**
  - Il est important que le commissaire aux comptes se renseigne sur la date prévisionnelle d'obtention de ce rapport afin d'apprécier si celle-ci est compatible avec l'organisation de ses travaux.
  - Une analyse détaillée du rapport d'assurance est à mener par le commissaire aux comptes notamment sur la nature de l'opinion, les éventuelles déviations identifiées dans le rapport et la période de couverture du rapport.

(2) ITGC : « Information Technology General Controls ».

(3) NEP 500 : Caractère probant des éléments collectés.

(4) Rapport portant une opinion d'audit et émis selon les normes en vigueur (par exemples la norme ISAE 3402 - International Standard on Assurance Engagements, la norme américaine SSAE18 – Statement on standards for attestation engagement AT- section 320).

(5) Le rapport d'assurance doit être communiqué au commissaire aux comptes par l'entité auditée.

❖ **Cas 2 :** Le commissaire aux comptes ne peut pas s'appuyer sur un rapport d'assurance, ce dernier peut mettre en œuvre des procédures d'audit alternatives, à savoir réaliser des procédures d'audit chez le prestataire(soit directement soit en faisant appel à un autre auditeur). Cette dernière option peut présenter des complexités de mise en œuvre notamment si l'entité auditée n'a pas prévu de clauses d'audit dans le contrat.

Lorsque le commissaire aux comptes n'a pas la possibilité de mettre en œuvre des procédures d'audit chez le prestataire, il conclut qu'il ne peut pas s'appuyer sur les contrôles généraux informatiques et adapte son approche d'audit en conséquence (cf. la fiche n°3).

IV - Incidence sur la démarche d'audit

Le commissaire aux comptes :

- communique les faiblesses identifiées au niveau approprié au sein de l'entité,
- évalue l'intérêt d'avoir recours à un auditeur spécialisé dans les systèmes informatiques pour conduire les procédures couvertes dans cette fiche.

CNCC

COMPAGNIE
NATIONALE DES
COMMISSAIRES AUX
COMPTES

www.cncc.fr