PROCESSUS D'IDENTIFICATION ET D'ÉVALUATION DES RISQUES : CONSEILS SUR LA MISE EN ŒUVRE DE LA NORME ISA 315 (RÉVISÉ EN 2019)

Vous recherchez des conseils sur la manière de mettre en œuvre de nouvelles ou autres exigences de la norme internationale d'audit (ISA) 315 (révisée en 2019) ? Vous êtes curieux de connaître la raison pour laquelle certaines des exigences de la norme ISA 35 (révisée en 2019) existent et comment elles favorisent la réalisation d'un audit efficace ? Consultez ce guide pour en savoir plus !

AVERTISSEMENT

Cet outil est conçu pour aider les professionnels dans la mise en œuvre de la norme ISA 315 (révisée en 2019), *Identification et évaluation des risques d'anomalies significatives*, sans toutefois être destiné à remplacer la lecture de la norme. L'outil n'aborde pas toutes les exigences de la norme ISA 315 (révisée en 2019), mais se concentre uniquement sur de nouvelles exigences particulières et certaines autres exigences.

En outre, un professionnel devrait se servir de cet outil dans le cadre de son jugement professionnel ainsi que des faits et circonstances de chaque audit particulier. Il convient également de noter que les exemples fournis ici ne sont pas exhaustifs et ne représentent pas tous les aspects relatifs à l'identification et l'évaluation des risques. Ils sont surtout présentés pour contribuer à guider l'auditeur dans certains scénarios spécifiques plutôt que dans toutes les situations qu'il pourrait rencontrer durant un audit.

L'IFAC décline toute responsabilité ou obligation qui pourrait découler, de façon directe ou indirecte, de l'utilisation et de l'application du présent outil.

Normes abordées

Norme ISA 315 (révisée en 2019), *Identification et évaluation des risques d'anomalies*

Date d'entrée en vigueur

Les modifications de la norme ISA 315 (révisée en 2019) sont applicables aux audits d'états financiers pour les périodes ouvertes à compter du 15 décembre 2021[1].

1 La norme ISA 315 (révisée en 2019) s'applique également aux audits réalisés dans le cadre de la norme ISA 805, *Audits d'états financiers isolés et d'éléments spécifiques, de comptes ou de postes spécifiques d'un état financier – Considérations particulières.* La norme ISA 315 (révisée en 2019) est adaptée selon les besoins aux circonstances, lorsqu'elle est appliquée aux audits d'une autre information financière historique.

Point focal de l'outil

Le guide d'application non obligatoire *Outil d'aide à la mise en œuvre à l'intention des auditeurs (Outil)* souligne l'adaptabilité de la norme en se concentrant sur les entités peu complexes (EPC)[2].

Forme et contenu de cet outil

Le texte qui suit présente une analyse sommaire du contenu de cet *outil* :

- Figure 1 : vue d'ensemble du processus d'identification et d'évaluation des risques de la norme ISA 315 (révisée en 2019).
  - Chaque étiquette de la **Figure 1** apparaît sous le caractère référence N1. Pour accéder à une section qui aborde un sujet particulier, cliquez sur l'étiquette concernée. Pour revenir à la Figure 1, cliquez directement à partir de chaque section. La position de chaque caractère référence de la Figure 1 indique la partie du processus d'identification et d'évaluation des risques à laquelle la question abordée se rapporte de manière principale.
- Une brève discussion sur les concepts fondamentaux sélectionnés sous-tendant le processus d'identification et d'évaluation des risques et la manière de l'appliquer, notamment :
  - Le processus d'évaluation des risques dynamique et itératif
  - Le jugement professionnel et le scepticisme professionnel
  - Adaptabilité
- Explications sur certaines :
  - Nouvelles exigences (questions N1 à N6)
    - Éclaircissement sur les nouvelles exigences (questions N1 à N6) peuvent inclure la manière dont elles se rapportent à d'autres exigences et des documents d'application qui ne sont pas nouveaux.
  - Autres exigences (questions O1 à O5)

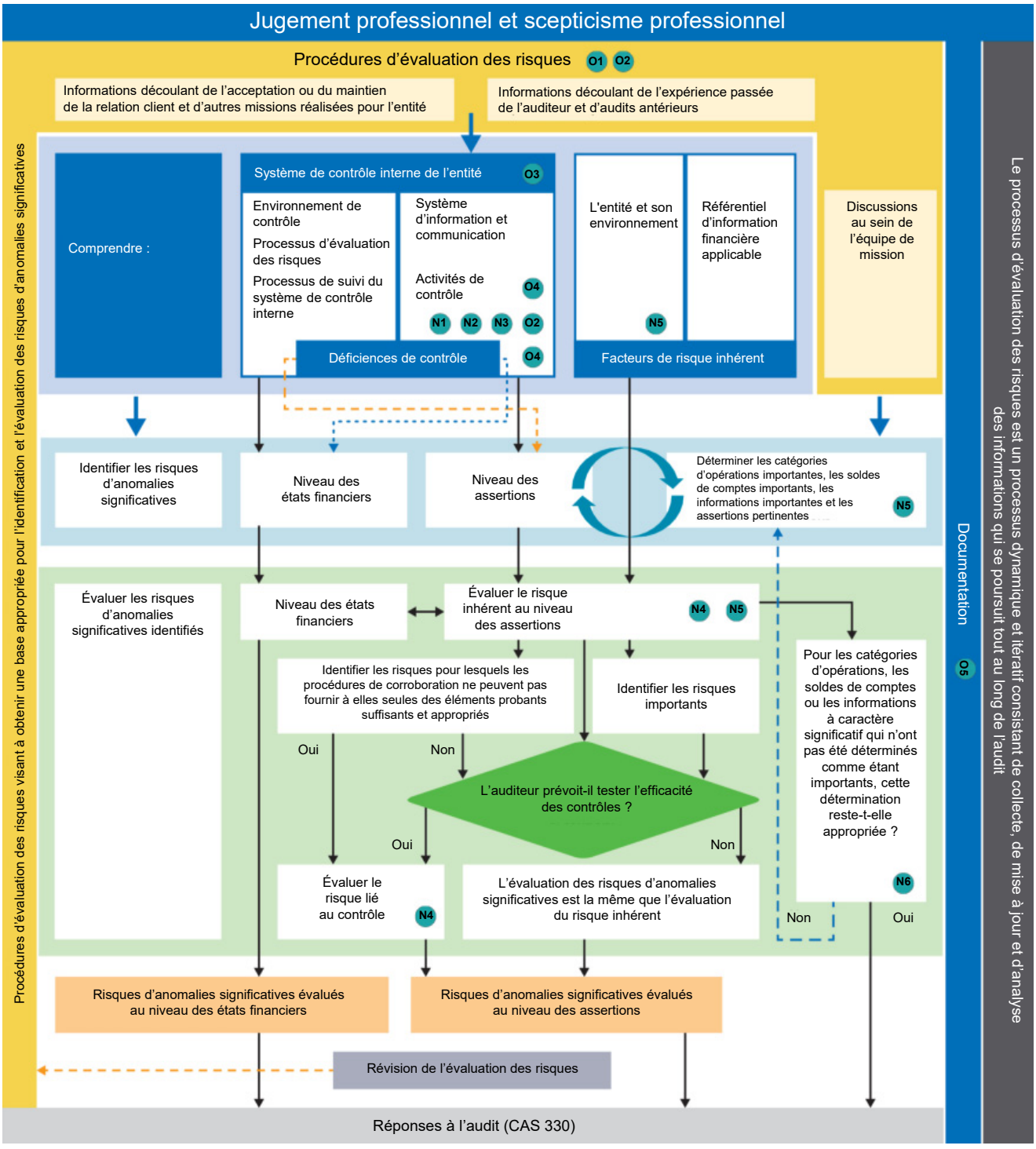
Remerciements

L'*outil* est fondé sur l'Outil d'aide à la mise en œuvre à l'intention des auditeurs des comptables professionnels agréés Canada (CPA Canada) et est utilisé avec l'autorisation de CPA Canada.

2 Les normes ISA ne donnent pas une définition de l'entité peu complexe (EPC). La norme ISA 315 (révisée en 2019) est applicable aux audits de toutes les entités, quelle que soit leur taille ou leur complexité. Le matériel d'application comprend donc des considérations spécifiques à la fois aux entités peu complexes et aux entités plus complexes, selon le cas. S'il est vrai que la taille d'une entité peut représenter un indicateur de sa complexité, il convient tout de même de noter qu'il existe de petites entités complexes ainsi que de grandes entités peu complexes. Le conseil international des normes d'audit et d'assurance (IAASB) propose actuellement un **projet** d'une nouvelle norme pour les audits des EPC fournissant un contexte supplémentaire à ce qui pourrait constituer une EPC.

Vue d'ensemble du processus d'identification et d'évaluation des risques de la norme ISA 315 (révisée en 2019)

Figure 1[3,4] : VUE D'ENSEMBLE DU PROCESSUS D'IDENTIFICATION ET D'ÉVALUATION DES RISQUES DE LA NORME ISA 315 (révisée en 2019)



3 Cette figure est un extrait de l'introduction à la norme ISA 315 (révisée en 2019) : *Identification et évaluation des risques d'anomalies significatives* du Conseil international des normes d'audit et d'assurance, publiée par la Fédération internationale des experts-comptables en décembre 2019.

4 La norme ISA 315 (révisée en 2019) est destinée aux audits de toutes les entités, quelle que soit leur taille ou leur complexité. Le matériel d'application et ce guide intègrent des considérations spécifiques aux entités peu complexes.

Concepts fondamentaux sélectionnés sous-tendant le processus d'identification et d'évaluation des risques

Objectif

La norme ISA 315 (révisée en 2019), *Identification et évaluation des risques d'anomalies*, a fait l'objet d'une importante révision. Les changements et les nouvelles exigences sont destinés à clarifier l'identification et l'évaluation des risques d'anomalies significatives et à vous aider à les réaliser d'une manière plus cohérente et plus solide. Une fois que les risques d'anomalies significatives sont identifiés et évalués, la norme ISA 330, *Réponses de l'auditeur à l'évaluation des risques*, exige la conception et la réalisation de procédures d'audit complémentaires afin de répondre à ces risques d'anomalies significatives d'une manière appropriée et de déterminer si vous avez obtenu des éléments probants appropriés suffisants. La qualité de votre processus d'identification et d'évaluation des risques (ci-après désigné « évaluation des risques ») revêt donc un effet généralisé sur tous les aspects de l'audit. L'acquisition d'une compréhension de l'entité et de son environnement, du référentiel d'information financière applicable ainsi que du système de contrôle interne de l'entité vous fournit un cadre de référence dans lequel vous identifiez et évaluez les risques d'anomalies significatives. Bien que cette norme ISA ait été soumise à une révision considérable, le modèle de risque d'audit et votre objectif consistant à identifier et à évaluer les risques d'anomalies significatives au niveau des états financiers et des assertions, qu'elles soient dues à une fraude ou à une erreur, demeure le même[5].

Processus d'évaluation des risques dynamique et itératif

La colonne de droite de la **Figure 1** indique que le processus d'évaluation des risques est dynamique et itératif. Vos évaluations préliminaires des risques, ainsi que les réponses planifiées à ces évaluations, peuvent avoir besoin d'être modifiées lors de l'obtention de nouvelles informations, au fur et à mesure de l'avancement de l'audit. Vous devez rester attentif à cette possibilité tout au long de l'audit. Cela peut inclure des changements touchant à la fois vos réponses globales et des procédures d'audit complémentaires. Le point essentiel est mis en évidence par l'inclusion de la case « révision de l'évaluation des risques » en bas de la figure.

Jugement professionnel et scepticisme professionnel

La norme ISA 200, *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux normes internationales d'audit* vous impose d'exercer votre jugement professionnel et de maintenir un scepticisme professionnel[6] tout au long de la planification et de la réalisation de l'audit, y compris pendant l'exécution des procédures d'évaluation des risques[7]. Par exemple, l'un des jugements que vous devez faire porte sur l'évaluation du degré d'importance d'un risque identifié (voir la question **N5**).

Des changements ont été apportés aux normes pour encourager l'auditeur à faire preuve d'un état d'esprit plus sceptique lors des procédures d'évaluation des risques. Il est important de souligner que lors de la conception et de la mise en œuvre des procédures d'évaluation des risques, il convient de procéder d'une manière impartiale, sans chercher à obtenir des éléments probants susceptibles d'être corroborés ni à exclure des éléments probants susceptibles d'être contradictoires. Cela pourrait vous permettre d'exercer un scepticisme professionnel lors de l'identification et de l'évaluation des risques d'anomalies significatives. Le scepticisme professionnel est une attitude adoptée lors de la formulation de jugements professionnels, qui sert ensuite de base à l'action.

5 La **Fiche d'information** Introduction à la norme ISA 315 (révisée en 2019) *Identification et évaluation des risques d'anomalies significatives* de l'IAASB comporte une vue d'ensemble des changements d'importance.

6 La norme ISA 200, *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux normes internationales d'audit*, définit le « jugement professionnel » et le « scepticisme professionnel ». Voir la norme ISA 200.13 (k) et (l).

7 La norme ISA 315.12 (j) définit les « procédures d'évaluation des risques », les procédures d'audit conçues et mises en œuvre pour identifier et évaluer les risques d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, au niveau des états financiers et au niveau des assertions.

Autrement dit, lors de l'exercice d'un scepticisme professionnel, vous ne cherchez pas uniquement à corroborer un chiffre présenté dans les états financiers. Vous pouvez exercer le scepticisme professionnel en :

- remettant en question des informations contradictoires ainsi que la fiabilité des documents ;
- examinant les réponses aux demandes d'informations et les autres renseignements obtenus auprès de la direction et des responsables de la gouvernance ;
- étant attentif aux conditions pouvant éventuellement dénoter des anomalies, que celles-ci soient le résultat de fraudes ou d'erreurs ;
- déterminant si les éléments probants obtenus étayent votre identification et évaluation des risques d'anomalies significatives, compte tenu de la nature et des circonstances de l'entité.

Adaptabilité

La norme ISA 315 (révisée en 2019) s'applique à l'audit des états financiers de toutes les entités, quelle que soit leur nature, leur taille, ou leur complexité. La norme ISA 315 (révisée en 2019) comprend quelques nouveaux paragraphes de matériels d'application (y compris des exemples) qui définissent des questions à prendre en compte lors de l'audit d'états financiers d'une entité peu complexe (EPC). Ces paragraphes sont identifiés par des en-têtes d'« adaptabilité ».

En général, les paragraphes d'adaptabilité vous fournissent un contexte sur l'application des exigences de la norme ISA 315 (révisée en 2019) à tous les types d'entités, peu complexes à complexes, et favorisent l'exercice du jugement professionnel pour déterminer les procédures d'audit que vous devez effectuer. De même, ces paragraphes rappellent utilement que les entités peu complexes peuvent utiliser des systèmes et des processus qui manquent de formalisme et que divers aspects du système de contrôle interne d'une entité peu complexe sont affectés par l'implication directe du propriétaire d'une entreprise ou du directeur général d'une organisation à but non lucratif (pour plus de simplicité, appelé « propriétaire » dans les exemples inclus dans cet *outil)*, tout en restant appropriés à la nature et aux circonstances de l'entité.

Remarque : cet *outil* aborde les diverses questions liées à l'adaptabilité. Les explications et les exemples présentés ci-dessous sont fournis dans un contexte d'audit d'états financiers d'une entité peu complexe.

Explication des nouvelles exigences

N1 – Pourquoi la norme ISA 315 (révisée en 2019) précise-t-elle dorénavant les contrôles que vous devez identifier afin de comprendre la composante « activités de contrôle » ?
(Norme ISA 315.26)

Dans la version précédente, il fallait identifier les « contrôles pertinents à l'audit ». Les contrôles spécifiques qu'il est nécessaire d'identifier ont été inclus dans diverses normes, ce qui a engendré des interprétations différentes et une pratique incohérente. Par conséquent, lors de la révision de la norme ISA 315 (révisée en 2019), l'IAASB a recueilli et regroupé tous les contrôles pertinents qu'il faut nécessairement comprendre afin d'identifier et d'évaluer les risques d'anomalies significatives et de savoir clairement quels contrôles sont soumis aux exigences de la composante « activités de contrôle ».

Retour à la **Figure 1**.

La compréhension de la composante « activités de contrôle » exige l'identification des contrôles qui portent sur les risques d'anomalies significatives au niveau des assertions.

Ceux-ci, lorsqu'ils existent, comprennent les éléments suivants :

1. des contrôles visant à répondre à un risque que vous déterminez comme étant important ;
2. des contrôles sur les écritures de journal, y compris les écritures non courantes servant à enregistrer les opérations ou ajustements non récurrents ou inhabituels ;
3. des contrôles dont vous prévoyez tester l'efficacité de fonctionnement dans l'identification de la nature, du calendrier et de l'étendue des procédures de corroboration (ces contrôles comprennent les contrôles visant à répondre aux risques pour lesquels les procédures de corroboration ne peuvent fournir à elles seules des éléments probants appropriés suffisants) ;
4. d'autres contrôles que vous jugez appropriés, en fonction de votre jugement professionnel, pour répondre aux objectifs d'obtention d'éléments probants fournissant une base appropriée pour :
   a. l'identification et l'évaluation des risques d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, au niveau des états financiers et au niveau des assertions ;
   b. la conception, conformément à la norme ISA 330, de procédures d'audit complémentaires.

- Des contrôles informatiques généraux pour répondre aux risques découlant du recours de l'entité à l'informatique.

D'autres normes internationales d'audit[8] exigent également l'identification des contrôles spécifiques suivants dans les composantes du contrôle interne, le cas échéant.

- Contrôles liés à l'information traitée par un organisme de services.
- Contrôles instaurés dans le cadre des relations avec les parties liées afin d'identifier, de comptabiliser et de publier conformément au référentiel d'information financière applicable, d'autoriser et d'approuver les opérations et accords importants avec les parties liées, et d'autoriser et d'approuver les opérations et accords importants en dehors du cours normal des activités.

Veuillez vous référer aux sous-paragraphes applicables dans la norme ISA 315.26 et aux paragraphes A147-A157 pour plus de détails sur les contrôles 1 à 5 susmentionnés. En outre, l'IAASB a élaboré le **Guide de première mise en œuvre de la norme ISA 315 (révisée en 2019)**, et les paragraphes 57 à 64 sont particulièrement utiles pour expliquer les contrôles identifiés dans la composante « activités de contrôle ».

8 La norme ISA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services* (paragraphe 10) et la norme ISA 550, Parties liées (paragraphe 14).

En ce qui concerne les contrôles que vous identifiez dans la composante « activités de contrôle », vous devez :

- évaluer si le contrôle est conçu pour gérer efficacement le risque d'anomalies significatives au niveau des assertions ou pour soutenir le fonctionnement d'autres contrôles, et
- si le contrôle a été mis en œuvre au moyen de procédures autres que les enquêtes menées auprès du personnel de l'entité.

Si vous estimez que ces contrôles ne sont pas conçus ou qu'ils n'ont pas été mis en œuvre de manière appropriée pour empêcher, ou pour détecter et corriger une anomalie significative, vous devez déterminer si ces déficiences constituent, individuellement ou collectivement, une déficience importante en vertu de la norme ISA 265, *Communication des déficiences du contrôle interne aux responsables de la gouvernance et à la direction*[9], et si vous pourriez avoir besoin de prendre en compte l'incidence de la déficience de contrôle sur la conception des procédures d'audit complémentaires en vertu de la norme ISA 330[10].

Se reporter à la question **O3** pour examiner la raison pour laquelle vous devez acquérir une compréhension de la composante « activités de contrôle » du système de contrôle interne de l'entité.

Se reporter à la question **O2** pour en savoir plus sur l'obtention d'éléments probants sur la conception et la mise en œuvre de contrôles dans les composantes « activités de contrôle ».

Les exemples suivants expliquent l'application du paragraphe 26 de la norme ISA 315 (révisée en 2019).

1. Contrôles visant à répondre à un risque que vous déterminez comme étant important

Tous les risques d'anomalies significatives dues à la fraude sont traités comme des risques importants ; il existe une présomption simple qu'il y a des risques de fraude dans la comptabilisation des recettes[11]. En outre, la comptabilisation des recettes peut également donner lieu à des risques importants non liés à la fraude.

Exemple 1

Un risque considérable d'anomalies significatives dans les recettes peut apparaître, par exemple, lorsqu'une entité peu complexe fournit des services en vertu de contrats dotés de termes complexes, y compris la nécessité de procéder à des estimations pour savoir quand il faut comptabiliser les recettes et quels montants il convient de comptabiliser. Le risque alors existant consisterait à ne pas comptabiliser les recettes durant la période appropriée et à avoir des montants comptabilisés d'une manière non conforme au référentiel d'information financière applicable. Dans ce cas, les processus associés aux tests de conception et de mise en œuvre des contrôles pourraient être liés (1) à la manière d'identifier les contrats, (2) à la détermination par un personnel qualifié de la manière de comptabiliser les contrats en vertu du référentiel d'information financière applicable et (3) aux obligations en matière de performance et les estimations de la direction, afin de s'assurer que les montants appropriés ont été enregistrés.

Exemple 2

L'entité peu complexe peut avoir conçu son système de comptabilité pour enregistrer les recettes des ventes de ses marchandises sur une base de point d'expédition FAB (franco à bord). En d'autres termes, selon les termes des contrats de vente, le transfert des risques de l'EPC à son client a lieu lorsque les marchandises quittent les locaux de l'entité peu complexe. Cependant, l'entité peu complexe peut également avoir des contrats de vente destination FAB. De cette manière, le transfert des risques et des récompenses nécessaire pour reconnaître les recettes a seulement lieu à la réception des marchandises par le client. Par conséquent, à la fin de l'exercice, les recettes peuvent être surestimées pour les marchandises expédiées sur une base de destination FAB qui n'auront pas encore été reçues par les clients. L'entité peu complexe a conçu un contrôle pour identifier toutes

9 Norme ISA 315.A183.

10 Norme ISA 315.A182.

11 Norme ISA 240, *Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers* (paragraphes 27-28).

les ventes à destination FAB dans lesquelles les marchandises ne sont pas encore arrivées à destination en fin d'année. En se fondant sur la durée moyenne d'arrivée à destination (environ deux semaines), le commis aux comptes clients obtient les informations des deux dernières semaines de ventes à destination FAB et effectue le rapprochement avec les informations fournies par le transporteur qui confirment la date d'arrivée à destination. Toutes les marchandises qui ne sont pas reçues avant la fin de l'année doivent faire l'objet d'une écriture de journal pour inverser la vente.

Lorsque l'auditeur a défini une opportunité de commettre une fraude en déplaçant les revenus vers la période en cours sans avoir satisfait au critère de comptabilisation des recettes, il doit examiner les facteurs de risque de fraude liés à l'incitation ou à la pression de commettre une fraude et au volume des ventes à destination FAB et déterminer s'il existe un risque de fraude dans la comptabilisation des recettes en raison de la possibilité de l'existence d'anomalies significatives. Le contrôle de « rapprochement par le commis aux comptes clients des ventes à destination FAB avec les informations fournies par le transporteur » serait ainsi identifié comme un contrôle approprié visant à gérer ce risque important.

2. **Contrôles sur les écritures de journal (y compris les écritures non courantes servant à enregistrer des opérations ou ajustements non récurrents ou inhabituels)**

   Étant donné qu'une entité transfère généralement les informations entre les systèmes de traitement des opérations et le grand livre général au moyen d'écritures de journal, courantes ou non, automatisées ou manuelles, tous les audits comportent des contrôles afférents aux écritures de journal. Il existe également un risque que des écritures de journal « non appropriées » soient utilisées pour remplacer des enregistrements valides ou pour manipuler les états financiers.

   Exemples spécifiques :

   a. Avoir une séparation de fonctions appropriée entre le préparateur et l'approbateur des écritures de journal manuelles

   b. Disposer de contrôles d'interface appropriés entre les sous-journaux et le grand livre pour les écritures d journal automatisées

   Se reporter à la question **N2** pour en savoir plus sur les contrôles appliqués sur les écritures de journal concernées par le paragraphe 26.

   Se reporter à la question **N3** pour une discussion et un exemple des contrôles informatiques généraux qu'il convient d'identifier en ce qui concerne les contrôles sur les écritures de journal.

3. **Contrôles dont vous prévoyez tester l'efficacité du fonctionnement dans l'identification de la nature, du calendrier et de l'étendue des procédures de corroboration**

   Vous pouvez être confronté à des circonstances dans lesquelles vous concluez que l'approche d'audit consistant à tester l'efficacité de fonctionnement d'un ou de plusieurs contrôles est susceptible d'être efficace et efficiente pour déterminer la nature, le calendrier et l'étendue des procédures de corroboration. Cette situation peut se poser, par exemple, lorsque le flux des opérations de recettes de l'entité peu complexe comprend un grand volume de petits montants homogènes.

   Par exemple, lors de la réalisation d'un audit des états financiers d'un commerce de proximité, vous pourriez déterminer que l'entité peu complexe a effectivement conçu et mis en œuvre des contrôles sur le processus des reçus automatisés au point de vente et de son processus de rapprochement des factures avec les dépôts bancaires comptabilisés. En résultat, vous pourriez conclure qu'il serait approprié de tester l'efficacité opérationnelle de ces contrôles afin de vous aider à concevoir vos procédures de corroboration, y compris la détermination de la portée des tests.

4. Autres contrôles que vous jugez appropriés, en fonction de votre jugement professionnel, pour répondre aux objectifs (voir les objectifs au point 4 ci-dessus)

Contrôles que vous pourriez juger appropriés pour répondre aux objectifs en matière d'obtention d'éléments probants fournissant une base appropriée pour l'identification et l'évaluation des risques et la conception de procédures d'audit complémentaires. Ceux-ci peuvent inclure des contrôles visant à répondre aux risques identifiés d'anomalies significatives qui se situent, selon votre évaluation, dans la partie supérieure de l'échelle de risque inhérent, mais qui n'ont pas été identifiés comme des risques importants. Ces contrôles peuvent être destinés, par exemple, à gérer les risques inhérents des casiers en rose sombre de la **Figure 3** (c'est-à-dire les risques liés à la combinaison d'une probabilité modérée / grande amplitude ou d'une probabilité élevée / amplitude modérée).

Par exemple, la nature des activités de l'entité peu complexe et les aspects de son système informatique peuvent entraîner le placement de divers éléments dans des comptes d'attente. En raison de la nature du compte d'attente, vous avez initialement déterminé que les comptes d'attente devaient être évalués comme présentant un risque inhérent plus élevé (mais pas un risque important) ; en d'autres termes, le risque d'anomalie significative est plus élevé dans le compte d'attente, sans pour autant constituer un risque important pour l'entité peu complexe. En vous fondant sur votre jugement professionnel, vous pouvez estimer que les politiques et procédures (c'est-à-dire les contrôles) relatives au suivi et à la régularisation en temps utile des éléments en suspens jouent un rôle important dans la prévention, la détection et la correction de toute anomalie significative susceptible de survenir. Vous identifiez les contrôles relatifs au rapprochement, à la régularisation et à l'examen des comptes d'attente, et les types d'activités liées à ces comptes qui peuvent être réalisées. Ces contrôles font partie de la composante « activités de contrôle ». Si vous estimez que ces contrôles ne sont pas conçus ou qu'ils n'ont pas été mis en œuvre de manière appropriée pour empêcher, ou pour détecter et corriger une anomalie significative, vous devrez déterminer si ces déficiences constituent, individuellement ou collectivement, une déficience significative en vertu de la norme ISA 265[12]. Si vous avez identifié une ou plusieurs déficiences de contrôle, vous pouvez étudier leur incidence sur la conception de procédures d'audit complémentaires conformément à la norme ISA 330[13], notamment la réalisation de procédures différentes ou plus poussées en ce qui concerne la disposition des éléments en suspens, et peut-être l'affectation d'un personnel plus expérimenté pour mener ces procédures. Cela vous permettra également d'identifier de nouveaux risques d'anomalies significatives ou d'évaluer le risque inhérent à un niveau plus élevé sur l'échelle des risques inhérents. Par exemple, vous pouvez avoir initialement déterminé que les comptes d'attente ne constituent pas un risque important ; cependant, après avoir obtenu les informations susmentionnées, vous pourriez conclure que la probabilité d'un risque d'anomalie significative est en fait plus élevée en l'absence de contrôles sur les comptes d'attente.

5. Contrôles généraux informatiques (CGI)

L'identification de ces contrôles généraux informatiques se fait en[14] :

a. identifiant les applications informatiques connexes et les autres aspects de l'environnement informatique de l'entité (par exemple, l'infrastructure et les processus informatiques) qui sont exposés à des risques liés à l'utilisation de cette technologie de l'information, et ce, **en se basant sur les contrôles identifiés aux points 1 à 4 du premier paragraphe de la présente section :**

b. identifiant les risques posés par l'utilisation par l'entité des systèmes informatiques dans ces applications et d'autres aspects de son environnement informatique identifiés dans la bulle ci-dessus ;

c. identifiant les contrôles généraux informatiques qui gèrent ces risques[15].

12 Norme ISA 315.A183.

13 Norme ISA 315.A182.

14 Norme ISA 315.26 (b)-(c).

15 La norme ISA 315.12 contient des définitions des contrôles généraux informatiques, de l'environnement informatique et des risques découlant de l'utilisation de l'informatique.

Les étapes ci-dessus ne sont pas forcément complexes, mais elles dépendent des contrôles identifiés aux points 1 à 4 du premier paragraphe de la présente section, de l'étendue et de la complexité des applications informatiques, des différentes couches de l'infrastructure informatique soutenant ces applications informatiques et des processus informatiques correspondants.

Par exemple, en ce qui concerne les contrôles liés aux comptes d'attente mentionnés au point (d) ci-dessus, il existe également des contrôles d'accès aux comptes d'attente (par exemple, qui a accès pour traiter les opérations de ce compte). Il peut s'agir d'un contrôle informatique général qui serait identifié pour l'objectif de cette exigence.

Voir la question **O4** pour un exemple de l'application des étapes susmentionnées à un logiciel commercial peu complexe.

En outre, l'annexe 6 de la norme ISA 315 (révisée en 2019) présente des exemples de contrôles généraux informatiques pour gérer certains risques posés par l'utilisation des systèmes informatiques.

N2 – Quels sont les contrôles d'écritures de journal concernées par la portée du paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) ?

Le paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) (dans la composante « activités de contrôle ») exige l'identification des contrôles afférents aux écritures de journal ; y compris les écritures de journal non courantes servant à enregistrer des opérations ou ajustements non récurrents ou inhabituels.

Il convient de faire preuve d'un jugement professionnel pour déterminer les écritures de journal pertinentes aux fins de l'identification des contrôles visés au paragraphe 26(a)(ii)[16] de la norme ISA 315 (révisée en 2019). Dans l'environnement actuel où les processus automatisés sont considérables, vous devrez établir des contrôles sur les écritures de journal qui doivent faire l'objet d'une attention particulière aux fins de l'application du paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019).

Retour à la **Figure 1.**

Le paragraphe 25 de la norme ISA 315 (révisée en 2019) exige une « compréhension du système d'information de l'entité et de la communication pertinente à la préparation des états financiers… » pour les catégories importantes d'opérations, les soldes de comptes et les informations à fournir, y compris « la manière de lancer les opérations, d'enregistrer, de traiter, de corriger si nécessaire et d'intégrer les informations qui les concernent dans le grand livre et de les rapporter dans l'état financier… »[17]. L'acquisition de cette compréhension vous fournira des connaissances sur le système d'information de l'entité et vous permettra ainsi d'identifier les écritures de journal et les contrôles afférents, que les écritures soient courantes ou non, automatisées ou manuelles. L'identification des écritures de journal et de leurs contrôles connexes représente ainsi un jugement basé sur la nature et les circonstances de l'entité, y compris son système d'information.

Le paragraphe 26(a)(ii) est axé sur les contrôles afférents aux écritures de journal qui gèrent un ou plusieurs risques d'anomalies significatives au niveau des assertions, et qui pourraient être susceptibles de faire l'objet d'une intervention ou d'une manipulation non autorisée ou inappropriée. Ces contrôles comprennent :

- Les contrôles afférents aux écritures de journal non courantes, que les écritures de journal utilisées pour enregistrer les opérations ou ajustements inhabituels et non récurrents soient automatisées ou manuelles.

16 Le paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) porte sur les *contrôles afférents aux écritures de journal* qui doivent être comprises dans le cadre de la compréhension du système de contrôle interne de l'entité. Le paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) porte à la fois sur la fraude et l'erreur et se concentre sur les contrôles afférents aux écritures de journal qui gèrent les risques d'anomalies significatives au niveau des assertions. Le paragraphe 33(a) de la norme ISA 240 exige qu'un auditeur teste la pertinence des écritures de journal en se concentrant spécifiquement sur les risques d'anomalies significatives dues à la fraude. L'exigence de la norme ISA 240 est axée sur les *tests afférents aux écritures de journal* et est sensible au risque de contournement des contrôles par la direction.

17 Norme ISA 315, paragraphe 25(a)(i)

- Les contrôles afférents aux écritures de journal courantes, où les écritures de journal sont automatisées ou manuelles et sont susceptibles de faire l'objet d'une intervention ou manipulation non autorisée ou inappropriée. Cela pourrait se produire, par exemple, dans le cas d'écritures automatisées, si des personnes n'ayant pas l'autorité nécessaire ont accès au code source ou parviennent à apporter des modifications inappropriées aux configurations (c'est-à-dire que l'écriture, bien qu'automatisée, peut faire l'objet de manipulations). Par contre, les contrôles sur les écritures de journal courantes automatisées, tels que les contrôles sur les écritures de journal générées par le système qui sont directement et systématiquement traitées dans le grand livre, ne justifieraient pas l'attention du paragraphe 26(a)(ii), car on estime que la probabilité d'une intervention ou d'une manipulation non autorisée ou inappropriée est faible ou inexistante et qu'elle ne donne donc pas lieu à un risque d'anomalie significative au niveau des assertions.

Vos évaluations relatives au risque inhérent sont réalisées sans tenir compte des contrôles de l'entité. Cela permet d'éviter, par exemple, de procéder à des évaluations inappropriées de risques plus faibles fondées sur des hypothèses ou de s'appuyer involontairement sur le fait que les contrôles fonctionnent efficacement, sans avoir évalué la conception et testé l'efficacité de leur fonctionnement.

N3 – Quels sont les contrôles généraux informatiques (CGI) qu'il faudrait identifier en matière de contrôles afférents aux écritures de journal à des fins de conception et de mise en œuvre (c'est-à-dire, afin de déterminer si un contrôle a été conçu et mis en œuvre de manière efficace). Par exemple, est-il nécessaire d'identifier un contrôle général informatique pour chaque contrôle afférent aux écritures de journal identifiées au paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) et de procéder à une conception et une mise en œuvre pour ce CGTI ?

Le paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) exige l'identification de contrôles spécifiques devant faire l'objet de conception et de mise en œuvre, y compris des contrôles afférents à des écritures de journal (voir **N2** pour connaître la portée des écritures de journal et des contrôles soumis à cette exigence). Si l'un de ces « contrôles identifiés » (par exemple, les contrôles visés au paragraphe 26(a)(i)-(iv)) implique le recours à l'informatique ou la dépendance d'un système informatique, vous êtes obligé (en vertu du paragraphe 26(b)) d'identifier l'application informatique associée et tout autre aspect de l'environnement informatique qui pourraient être sujets à risque en raison du recours à l'informatique[18]. Vous devez ensuite identifier les risques associés découlant de l'utilisation de l'informatique et les contrôles généraux informatiques qui gèrent ces risques, puis procéder à une conception et une mise en œuvre sur ces contrôles généraux informatiques.

Retour à la **Figure 1**.

Lors de l'identification des contrôles généraux informatiques qui feront l'objet d'une procédure de conception et de mise en œuvre, le matériel d'application justificatif explique que l'identification des risques découlant du recours à l'informatique ne concerne que les applications informatiques identifiées, ou d'autres aspects de l'environnement informatique, pour les contrôles de la composante « activités de contrôle » (comme indiqué au paragraphe 26(b) de la norme ISA 315 (révisée en 2019)).

Tous les contrôles afférents à une écriture de journal générée par un système qui ont été identifiés au paragraphe 26(a)(ii) de la norme ISA 315 (révisée en 2019) ne doivent pas nécessairement être assortis de contrôles généraux informatiques connexes exigeant une procédure de conception et de mise en œuvre. Les contrôles généraux informatiques sont plutôt pris en compte selon leur pertinence aux risques découlant du recours à l'informatique pour les applications informatiques ou d'autres aspects de l'environnement informatique pour les contrôles identifiés dans le paragraphe 26(a)(i)-(iv) de la norme ISA 315 (révisée en 2019). L'identification de ces contrôles généraux informatiques soumis à une procédure de conception et de mise en œuvre représente un jugement basé sur la nature et les circonstances de l'entité, y compris ses systèmes d'information.

18 *Les risques découlant du recours à l'informatique* sont un terme défini dans le paragraphe 12(i) de la norme ISA 315 (révisée en 2019).

Exemple 1

L'entité peu complexe possède différentes couches de technologies de l'information utilisées dans son environnement informatique, depuis les applications informatiques proprement dites jusqu'à l'infrastructure informatique qui sous-tend ces applications, comme le réseau, le système d'exploitation, les bases de données et le matériel et logiciel associés. L'entité peu complexe peut avoir configuré ses systèmes de manière à ce que chaque employé doive saisir un mot de passe pour accéder à son système d'exploitation (accès à la couche réseau), qui donne ensuite accès à toutes les applications informatiques de l'entité (accès à la couche application). L'auditeur a identifié le contrôle consistant à définir des mots de passe pour se connecter aux différents systèmes d'exploitation (contrôle de la couche réseau) comme un contrôle général informatique présentant un risque lié à l'utilisation de l'informatique, au lieu des contrôles consistant à définir des mots de passe pour chaque application individuelle utilisée par l'entité (contrôle de la couche application).

N4 – Pourquoi devez-vous évaluer séparément le risque inhérent pour les risques d'anomalies significatives au niveau des assertions ? (Norme ISA 315.31 et .34)

Une évaluation séparée du risque inhérent améliore la qualité de votre processus d'évaluation des risques et permet de concentrer les efforts de l'auditeur pour répondre à l'évaluation des risques de façon appropriée. Lorsque vous élaborez vos procédures en réponse à l'évaluation du risque d'anomalies significatives, il faut prendre en considération les raisons de l'évaluation du risque d'anomalies significatives (RoMM) au niveau des assertions, y compris le risque inhérent et le risque lié au contrôle, et concevoir et mettre en œuvre des procédures appropriées.

Retour à la **Figure 1**.

Vos évaluations relatives au risque inhérent sont réalisées sans tenir compte des contrôles de l'entité. Cela permet d'éviter, par exemple, de procéder à des évaluations inappropriées de risques plus faibles fondées sur des hypothèses ou de s'appuyer involontairement sur le fait que les contrôles fonctionnent efficacement, sans avoir évalué la conception et testé l'efficacité de leur fonctionnement.

Bien qu'il vous incombe toujours d'évaluer le risque inhérent pour les risques identifiés d'anomalies significatives au niveau des assertions, vous n'êtes pas obligé d'évaluer le risque du contrôle que si vous prévoyez de tester l'efficacité de fonctionnement des contrôles ou si les procédures de corroboration ne suffisent pas à fournir des éléments probants suffisants et appropriés au niveau des assertions. Si vous ne prévoyez pas de tester l'efficacité du fonctionnement des contrôles, votre évaluation des risques de contrôle est telle que l'évaluation du risque d'anomalies significatives sera identique à celle du risque inhérent.

Bien que la réalisation d'évaluations séparées du risque inhérent et du risque de contrôle soit une nouvelle exigence (vu qu'elle ne peut plus être réalisée simultanément) de la norme ISA 315 (révisée en 2019), de nombreux auditeurs procédaient déjà à des évaluations séparées du risque inhérent et du risque de contrôle. Cela dit, si la méthodologie d'audit de votre entreprise dans le cadre de la norme ISA 315 (révisée) en vigueur comprenait des évaluations simultanées, ce changement s'appliquera à vous.

Les aspects du processus d'évaluation des risques inhérents sont abordés dans la question N5.

N5 – Pour les « facteurs de risque inhérent », la « probabilité et l'ampleur des anomalies » et l'« échelle de risque inhérent » sont-elles importantes dans la réalisation d'évaluations séparées du risque inhérent ? (Norme ISA 315.19(c) et 31-32)

Ces concepts vous permettent de mener une évaluation des risques plus ciblée et de meilleure qualité. Ainsi, votre réponse aux risques identifiés et évalués sera également plus ciblée sur ces derniers, ce qui contribuera à améliorer la qualité de l'audit.

Retour à la **Figure 1**.

Les « facteurs de risque inhérent », qui sont nouveaux dans la norme ISA 315 (révisée en 2019), sont des caractéristiques d'événements ou de situations qui affectent la possibilité qu'une assertion portant sur une catégorie d'opérations, un solde de compte ou une information à fournir comporte une anomalie, que celle-ci résulte d'une fraude ou d'une erreur, avant la prise en considération des contrôles. Les facteurs de risque inhérent se caractérisent par la complexité, la subjectivité, le changement, l'incertitude ou la susceptibilité à des anomalies en raison d'un parti pris de la direction ou d'autres facteurs de risque de fraude, dans la mesure où ils affectent le risque inhérent[19].

Il vous incombe[20] de tenir compte des facteurs de risque inhérent lors de la compréhension de l'entité et de son environnement et du référentiel d'information financière applicable et de les utiliser pour vous aider à identifier les risques d'anomalies significatives. Vous devez ensuite[21] tenir compte de la manière dont les facteurs de risque inhérent affectent la sensibilité des assertions concernées aux anomalies, et du degré de cette incidence, lors de l'évaluation du risque inhérent pour les risques identifiés d'anomalies significatives (c'est-à-dire les utiliser pour déterminer si un risque identifié se situe sur l'échelle de risque inhérent).

Vous n'êtes pas tenu de documenter la manière dont chaque facteur de risque inhérent a été pris en compte pour chaque catégorie d'opération, solde de compte ou information. Toutefois, la documentation de l'audit doit être suffisante pour permettre à un auditeur expérimenté, n'ayant aucune relation antérieure avec l'audit, de comprendre les questions importantes soulevées au cours de l'audit, les conclusions qui en découlent et les jugements professionnels significatifs portés pour parvenir à ces conclusions[22]. Lorsque l'auditeur « rend une question en considération », il pense consciemment à une chose lorsqu'il forme un jugement à propos d'une situation. Cela signifie que lorsqu'il acquiert la compréhension requise, l'auditeur réfléchit activement à la manière dont les facteurs de risque inhérent peuvent influencer l'information financière de l'entité, mais qu'il ne prend aucune mesure sauf si le facteur de risque inhérent est applicable. Il s'agit d'un processus itératif.

Pour chaque risque d'anomalie *significative* identifié au niveau des assertions, vous devez :

- Évaluer le risque inhérent en déterminant la probabilité et l'ampleur d'une anomalie, en tenant compte de la manière dont ces facteurs de risque inhérent affectent la susceptibilité des assertions concernées à des anomalies, et du degré de cette incidence.
- Tenir compte de la manière dont les risques d'anomalies significatives au niveau des états financiers affectent l'évaluation du risque inhérent, et de la mesure dans laquelle ils le font.
- Déterminer si les risques évalués d'anomalies significatives représentent des risques importants (c'est-à-dire des risques proches de l'extrémité supérieure de l'échelle du risque inhérent).

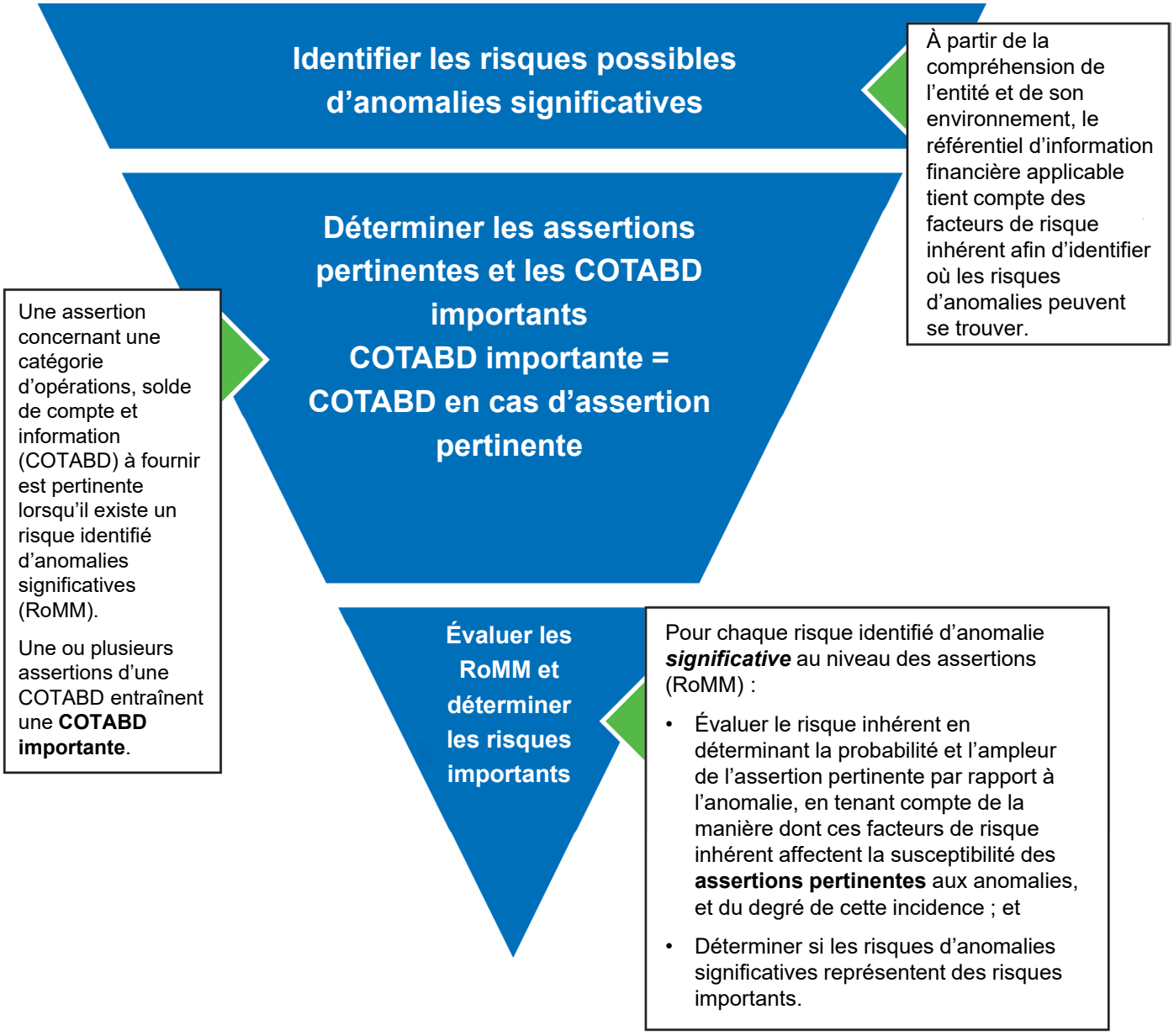
19 L'annexe 2 de la norme ISA 315 (révisée en 2019) fournit des descriptions des facteurs de risque inhérent et des questions à prendre en compte lors de leur compréhension et application.

20 Norme ISA 315.19(c).

21 Norme ISA 315.31(a).

22 Norme ISA 230, *Documentation de l'audit*, paragraphe 8(c).

FIGURE 2 – IDENTIFICATION ET ÉVALUATION DES RISQUES D'ANOMALIES SIGNIFICATIVES AU NIVEAU DES ASSERTIONS



* COTABD : catégories d'opérations, soldes de comptes et informations à fournir.

L'échelle de risque inhérent

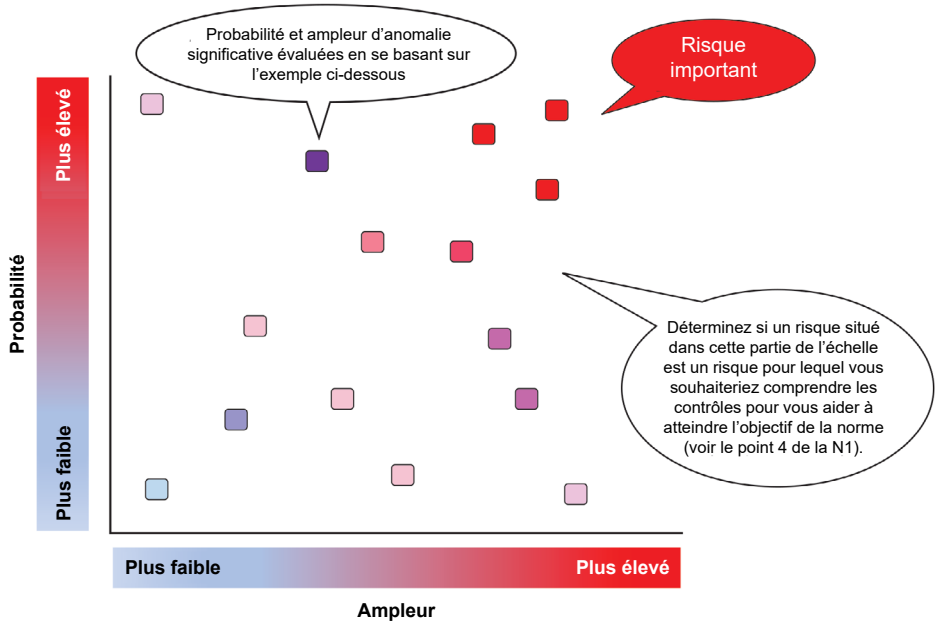
Le degré de variation du risque inhérent sur une échelle est désigné par l'expression « échelle de risque inhérent ». La figure 3 montre un exemple de la manière d'afficher une échelle de risque inhérent.

Pour chaque risque identifié d'anomalies significatives au niveau des assertions, vous devez évaluer la probabilité et l'ampleur de l'anomalie significative. Il s'agit de la combinaison de la probabilité et de l'ampleur qui déterminera où le risque inhérent est évalué sur l'échelle de risque inhérent.

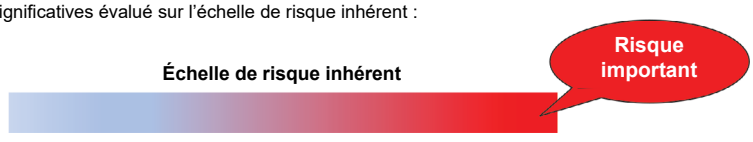
Votre estimation de la probabilité tient compte de la possibilité de survenance d'une anomalie, en fonction de la manière dont les facteurs de risque inhérent influencent le risque d'anomalie significative (par exemple, plus la complexité est importante, plus le risque identifié d'anomalies significatives sera susceptible de se situer à un niveau élevé sur l'échelle de risque inhérent).

Votre évaluation de l'ampleur d'une anomalie doit tenir compte à la fois des aspects qualitatifs et quantitatifs de l'éventuelle anomalie. Par exemple, le fait de déterminer si un risque d'anomalie lié à la classification est significatif peut nécessiter l'évaluation de considérations qualitatives, telles que l'effet d'une petite anomalie de classification sur le respect par l'entité peu complexe d'une convention d'endettement ou d'autres engagements contractuels. Une convention d'endettement peut inclure une exigence que l'entité peu complexe maintienne, au moins, un montant minimum de fonds de roulement. Une petite anomalie affectant le fonds de roulement peut avoir des conséquences importantes pour l'entité peu complexe si la correction de l'anomalie se traduit par un fonds de roulement inférieur au minimum spécifié dans la convention d'endettement. Par conséquent, le risque d'anomalies significatives lié à la classification peut exister, même si le montant de l'anomalie est d'une ampleur quantitative moins importante.

FIGURE 3 : EXEMPLE DE L'ÉVALUATION DE LA PROBABILITÉ ET DE L'AMPLEUR DES ANOMALIES EN DÉTERMINANT OÙ LE RISQUE INHÉRENT EST ÉVALUÉ SUR L'ÉCHELLE DE RISQUE INHÉRENT



☐ Chaque case représente une évaluation de risque inhérent différente pour une évaluation de risque identifié important. Elle représente une combinaison de l'évaluation de l'ampleur et de la probabilité d'une anomalie utilisée pour évaluer ce risque inhérent, en tenant compte des facteurs de risque inhérents. Chaque combinaison est utilisée pour déterminer le niveau d'un risque identifié d'anomalies significatives évalué sur l'échelle de risque inhérent :



Lors de l'évaluation du risque inhérent, vous devez exercer votre jugement professionnel pour déterminer l'importance de la combinaison formée par la probabilité et l'ampleur d'une anomalie[23]. Ce jugement peut dépendre de la nature, de la taille et de la complexité de l'entité, et tient compte de l'évaluation de la probabilité et de l'ampleur des anomalies ainsi que des facteurs de risque inhérent.

Exemple illustratif de l'application des questions indiquées dans les figures 2 et 3

Cet exemple est à titre indicatif et ne comprend que certains faits et circonstances afin de démontrer l'application de certaines exigences de la norme ISA 315 (révisée en 2019).

Le principal actif d'une entité peu complexe réside dans sa propriété immobilière constituée de terrains vacants, qui sont détenus en vue d'un développement futur et d'une vente éventuelle. L'entité peu complexe prépare des états financiers conformément à un cadre d'information financière en s'en servant d'un modèle de coût pour comptabiliser l'acquisition, la construction ou le développement dans le temps des biens immobiliers. Le cadre d'information financière exige que l'entité procède à un test de recouvrement lorsque des événements ou des changements de circonstances laissent à penser que la valeur comptable pourrait ne pas être recouvrable. Une perte de valeur est comptabilisée lorsque la valeur comptable n'est pas recouvrable et que la valeur comptable devient supérieure à la juste valeur.

La plupart des terrains vacants détenus par l'entité peu complexe se situent dans des régions géologiquement stables. Cependant, certaines de ses propriétés immobilières (environ 10 %) se trouvent sur les rivages et les collines sensibles à l'érosion. Au cours des dernières années, certaines régions ont connu des événements importants liés au changement climatique dans les régions côtières et montagneuses. En outre, certaines municipalités/régions envisagent de modifier le classement de certaines zones situées sur le rivage et à flanc de colline. L'entité peu complexe a déterminé qu'il y avait des événements ou des changements de circonstances pouvant indiquer que la valeur comptable des biens immobiliers pourrait ne pas être recouvrable.

Susceptibilité des assertions aux anomalies

L'auditeur estime que l'assertion relative à l'évaluation des biens immobiliers est susceptible de comporter des anomalies significatives. Cela pourrait affecter la valeur comptable du terrain vacant enregistrée dans le bilan et la perte de valeur enregistrée dans le compte de résultats, ainsi que les informations correspondantes.

Identification des risques d'anomalies significatives et assertions pertinentes

Étant donné que le terrain vacant constitue l'actif principal de l'entité peu complexe et que divers événements et conditions indiquent un changement possible de la valeur recouvrable du bien immobilier, l'auditeur identifie un risque d'anomalies significatives lié à l'estimation de la valeur recouvrable et, le cas échéant, de la juste valeur.

Par conséquent, l'auditeur identifie l'assertion relative à l'évaluation des biens immobiliers comme étant une assertion pertinente, puisqu'elle est associée à un risque d'anomalies significatives.

L'auditeur identifie la valeur comptable du terrain vague enregistrée dans le bilan, la perte de valeur enregistrée dans le compte de résultat, ainsi que les informations correspondantes, comme des catégories de transactions, de soldes de comptes et d'informations significatives parce qu'elles contiennent des assertions pertinentes.

Évaluation des risques d'anomalies significatives – risque inhérent

En ce qui concerne le risque d'anomalies significatives lié à l'estimation de la valeur recouvrable et, le cas échéant, de la juste valeur. L'auditeur estime le risque inhérent en évaluant la probabilité et l'ampleur et en prenant en considération la manière dont les facteurs de risque inhérent affectent la susceptibilité que l'assertion relative à l'évaluation comporte des anomalies et le degré de celles-ci.

23 Norme ISA 315.A208.

Compte tenu du changement ayant besoin d'un examen plus approfondi de la valeur recouvrable, les facteurs de risque inhérent qui affectent principalement la susceptibilité de l'assertion relative à l'évaluation de comporter une anomalie (que l'auditeur a déterminée pour cet exemple particulier) sont : la complexité (du calcul de la juste valeur (ou de la valeur recouvrable), la subjectivité (des données utilisées pour le calcul de la juste valeur (ou de la valeur recouvrable)) et l'incertitude (quant à ce qui pourrait se produire à l'avenir en ce qui concerne la valeur de l'actif et de sa valeur recouvrable).

Dans le cadre des changements des événements et des conditions, l'auditeur détermine qu'il existe un degré plus élevé de complexité, de subjectivité et d'incertitude.

Bien que la probabilité d'une anomalie significative soit plus élevée (en raison de la complexité, de la subjectivité et de l'incertitude), l'ampleur de l'anomalie potentielle peut ne pas être aussi significative, car seuls 10 % des biens immobiliers peuvent être exposés à un risque. En conséquence, le risque d'anomalies significatives est considéré comme étant plus élevé sur l'échelle de risque inhérent, sans toutefois constituer un risque important.

Évaluation des risques d'anomalies significatives – risque important (changements des faits)

Si les faits exposés ci-dessus étaient différents, par exemple, si les biens immobiliers sur le rivage et les collines sensibles à l'érosion représentaient 75 % des terrains vacants détenus par l'entité (au lieu de représenter environ 10 % comme décrit ci-dessus), l'ampleur d'une anomalie potentielle pourrait être plus significative. L'évaluation de la probabilité d'une anomalie n'a pas changé ; par conséquent, l'auditeur détermine le risque d'anomalies significatives lié à l'estimation du montant recouvrable et, le cas échéant, de la juste valeur (par exemple, l'évaluation de la valeur est une assertion pertinente, et la valeur comptable du bien et la perte de valeur sont des catégories d'opérations, soldes de comptes et informations à fournir importants) comme étant proche de la limite supérieure de l'échelle de risque inhérent (par exemple, voir « Risque important » mis en évidence dans la **Figure 3**).

N6 – Pourquoi faut-il procéder à une évaluation des risques en prenant du recul et comment cela se rapporte-t-il à l'obligation de réaliser des procédures de corroboration pour chaque catégorie significative d'opérations, de soldes de comptes et d'informations fournies dans la norme ISA 330.18 ? (Normes ISA 315.36, ISA 315.37)

L'évaluation des risques est un processus itératif. Une évaluation des risques en prenant du recul est destinée à favoriser une évaluation de l'exhaustivité des risques d'anomalies significatives qui ont été identifiés. Le recul est axé sur la question de savoir s'il existe des éléments dans la compréhension de l'auditeur qui peuvent indiquer l'existence d'autres risques d'anomalies significatives qui n'ont pas été identifiés dans les procédures déjà mises en œuvre.

En outre, si de nouvelles informations sont révélées au cours de l'audit, (1) pouvant affecter les risques d'anomalies significatives identifiés en raison de leur incohérence avec les éléments probants sur lesquels vous avez initialement fondé votre identification, ou (2) pouvant entraîner l'identification d'un nouveau risque d'anomalies significatives, il faudra réexaminer les évaluations des risques effectuées à l'origine et les réponses planifiées à ces risques.

Cela pourrait avoir des répercussions importantes sur la nature, le calendrier et l'étendue des procédures que vous effectuez pour répondre aux risques identifiés d'anomalies significatives.

Lorsque vous effectuez une évaluation des risques en prenant du recul, vous pourriez trouver une ou plusieurs catégories d'opérations, de soldes de comptes ou d'informations significatives que vous n'aviez pas jugés importants parce que vous n'aviez pas identifié de risques d'anomalies significatives liés aux assertions dans ces catégories d'opérations, de soldes de comptes ou d'informations à fournir. Ces catégories d'opérations, de soldes de comptes ou d'informations significatives doivent être réexaminées afin de confirmer l'absence de tout risque d'anomalies significatives. Même si aucun autre risque d'anomalies significatives n'est identifié, la norme ISA 330 (paragraphe 18) requiert toujours des procédures de corroboration sur ces catégories d'opérations, de soldes de comptes ou d'informations significatives.

Retour à la **Figure 1**.

Questions à poser lors d'une évaluation en prenant du recul

Les questions que vous pouvez envisager de vous poser en vue de déterminer si votre décision initiale reste appropriée comprennent, par exemple, la question de savoir si de nouvelles informations ont été communiquées sur les points suivants :

- Aspects de l'entité et de son environnement (par exemple, une acquisition commerciale qui change la structure organisationnelle, un changement dans le modèle d'entreprise tel que le lancement d'un nouveau produit, de nouvelles exigences réglementaires, des changements dans l'industrie)
- Les méthodes comptables de l'entité (par exemple, la modification de la méthode d'évaluation des stocks d'une méthode du coût moyen à une méthode premier entré, premier sorti)
- Comment et dans quelle mesure les facteurs de risque inhérent affectent la susceptibilité aux anomalies (par exemple, une utilisation accrue de feuilles de calcul complexes pour élaborer une provision ou une plus grande incertitude liée aux résultats d'un événement).
- Composantes de contrôle interne (par exemple, la perte d'employés de direction clé ou mise en œuvre d'un nouveau module logiciel)

Si les nouvelles informations obtenues ne sont pas cohérentes avec les éléments probants sur lesquels vous avez initialement fondé l'identification ou l'évaluation des risques d'anomalies significatives, vous devez déterminer s'il y a lieu de revoir le caractère significatif. La révision du caractère significatif peut également affecter votre identification des risques d'anomalies significatives.

Toutefois, il a été clairement établi qu'il n'est pas nécessaire de tester toutes les assertions appartenant à une catégorie significative de transactions, de soldes de comptes ou d'informations à fournir. En effet, en concevant les procédures de corroboration à mettre en œuvre, vous devez examiner la ou les assertions pour lesquelles une anomalie pourrait raisonnablement être significative si elle se produisait. Cela pourrait vous permettre de déterminer la nature, le calendrier et l'étendue des procédures à mettre en œuvre. Par exemple, l'entité peu complexe peut détenir un terrain et des bâtiments à leur coût d'acquisition, sans indication de dépréciation, pour lesquels vous n'avez pas identifié de risque d'anomalie significative. Lors des procédures de corroboration sur ce solde, vous pouvez décider de concevoir des procédures pour tester l'assertion d'existence.

Explications relatives à certaines autres exigences

O1 – Pourquoi devez-vous réaliser des procédures analytiques lors de l'identification et de l'évaluation des risques d'anomalies significatives ? (Norme ISA 315.14b)

Procédures analytiques :

- Permettent d'identifier les incohérences, les opérations ou événements inhabituels et les montants, ratios et tendances qui peuvent vous aider à identifier les risques d'anomalies significatives, particulièrement ceux qui sont dus à la fraude.
- Permettent d'identifier des aspects de l'entité dont vous n'aviez pas conscience afin de vous aider à identifier les risques d'anomalies significatives.
- Permettent de comprendre dans quelles mesures les facteurs de risque inhérent, tels que le changement, affectent la susceptibilité des assertions aux anomalies, ce qui peut aider l'auditeur dans l'évaluation des risques d'anomalies significatives.

Retour à la **Figure 1**.

Lorsque des procédures analytiques sont utilisées comme procédures d'évaluation des risques, il n'est pas nécessaire de les réaliser conformément aux dispositions de la norme ISA 520, *Procédures analytiques*[24], qui porte sur les procédures analytiques utilisées à des fins de corroboration et sur celles qui sont réalisées vers la fin de l'audit. Toutefois, les exigences et le matériel d'application de la norme ISA 520 peuvent fournir des indications utiles pour la mise en œuvre de procédures analytiques dans le cadre des procédures d'évaluation des risques. Les procédures analytiques peuvent être de simples comparaisons d'informations, comme la comparaison des soldes de l'exercice en cours avec ceux de l'exercice précédent[25]. Toutefois, les types de procédures analytiques utilisées précédemment peuvent ne pas être nécessairement efficaces pour l'identification et l'évaluation des risques d'anomalies significatives dans l'exercice en cours. En vous appuyant sur les connaissances acquises dans le cadre de votre compréhension de l'entité et de son environnement, du référentiel d'information financière applicable et du système de contrôle interne de l'entité, vous pouvez formuler des attentes sur la manière dont vous estimez que les soldes auraient dû évoluer. Par exemple, il se peut que de nouvelles transactions, de nouveaux événements ou de nouvelles conditions d'importance affectant l'activité ou l'information financière de l'entité aient eu lieu pendant l'année en cours et pour lesquels vous prévoyez de constater des changements, ou non, d'une année sur l'autre. Envisagez de vous demander, par exemple, dans quelle mesure une catégorie de transactions, un solde de compte ou une information à fournir auraient dû changer par rapport à la période précédente, compte tenu de votre compréhension actualisée de la situation.

Dans la mesure du possible, vous pourriez décider d'attendre avant de mettre en œuvre des procédures analytiques en tant que procédures d'évaluation des risques, jusqu'à ce que la comptabilité soit finalisée de telle sorte que les informations ne soient plus préliminaires. Par exemple, lorsque l'entité peu complexe aura effectué ses procédures de fin de période et développé diverses estimations (par exemple, amortissement, provision pour créances douteuses, etc.)

Cependant, même les informations préliminaires peuvent contribuer à corroborer ou à contredire les résultats des enquêtes sur les résultats d'exploitation, les performances financières et la situation financière. Les procédures analytiques fondées sur les informations préliminaires sont plus susceptibles d'aboutir à des comparaisons significatives lorsque l'information de l'exercice en cours est à peu près au même stade d'achèvement que l'information utilisée pour la période précédente.

24 Norme ISA 520, *Procédures analytiques*.

25 Norme ISA 315.A29.

O2 – Pourquoi devez-vous utiliser une combinaison de demandes d'informations, d'observations et d'inspections pour mettre en œuvre les procédures d'évaluation des risques, notamment pour obtenir des éléments probants sur la conception et la mise en œuvre des contrôles identifiés dans la composante « activités de contrôle » ?

(Norme ISA 315.13, .14, .19(a)-(b), .21-.26 et .A177)

L'observation et l'inspection peuvent permettre de corroborer ou de contredire les réponses aux demandes d'information de la direction et d'autres parties sur votre compréhension de l'entité et de son environnement, du référentiel d'information financière applicable et du système de contrôle interne de l'entité, notamment la composante « activités de contrôle ». Cette combinaison permet d'obtenir des éléments probants qui fournit une base appropriée à l'identification et l'évaluation des risques d'anomalies significatives.

La méthode adoptée par la direction pour concevoir et mettre en œuvre les contrôles dans la composante « activités de contrôle » permet d'acquérir une compréhension préliminaire de la manière selon laquelle l'entité identifie et gère les risques liés à l'activité. Elle peut également influencer de plusieurs manières l'identification et l'évaluation de l'auditeur des risques d'anomalies significatives et fournir une fondation pour votre conception et application des procédures de corroboration. La mise en œuvre d'un contrôle est déterminée par l'établissement de son existence, et du fait qu'une entité l'utilise conformément à sa conception. Toutefois, la seule demande d'informations en vue d'obtenir des éléments probants concernant la conception et la mise en œuvre des contrôles identifiés de la composante « activités de contrôle » n'est pas suffisante.

(Voir la question **N5** pour les contrôles spécifiés dans la norme ISA 315.26 pour lesquels vous devez évaluer la conception et déterminer la mise en œuvre.)

Retour à la **Figure 1**.

Procédures d'évaluation des risques (demande d'informations, observation et inspection)

Il est vrai que vous êtes tenu[26] de réaliser tous les types de procédures d'évaluation des risques (demandes d'informations auprès de la direction et d'autres personnes appropriées au sein de l'entité, procédures analytiques, observation et inspection) pour acquérir les connaissances requises sur l'entité et son environnement, le référentiel d'information financière applicable et le système de contrôle interne de l'entité, mais vous n'êtes pas obligé de les effectuer tous pour chaque aspect de cette compréhension. Il existe d'autres procédures qui peuvent être réalisées dans le cadre de l'acquisition de vos connaissances de l'entité et qui pourraient s'avérer utiles pour l'identification et l'évaluation des risques d'anomalies significatives. On peut citer, par exemple, les demandes d'informations auprès de personnes externes à l'entité, comme un conseiller juridique externe de l'entité ou des superviseurs externes, ou auprès d'experts en évaluation auxquels l'entité a fait appel.

Compréhension de l'entité et de son environnement

À titre d'exemple, les résultats de vos demandes d'informations peuvent révéler que l'entité n'a pas de nouvelles parties liées. L'inspection de la liste des fournisseurs importants comparée à celle de l'année précédente peut révéler l'existence d'un ou de plusieurs nouveaux fournisseurs importants. Lorsque vous parvenez à comprendre, par exemple, la nature, les montants, le calendrier et l'étendue des opérations de l'entité peu complexe avec ces nouveaux fournisseurs, vous pourrez identifier des conditions commerciales inhabituelles avec un fournisseur ainsi que d'autres facteurs indiquant qu'il s'agit d'une partie liée jamais identifiée auparavant. De ce fait, vous pourriez évaluer le risque d'anomalies significatives comme étant plus élevé que si vous n'aviez pris en compte que les demandes d'informations comme fondement de votre évaluation des risques.

26 Norme ISA 315.14.

Compréhension du référentiel d'information financière applicable

À titre d'exemple, les résultats de vos demandes d'informations peuvent indiquer que l'entité maintient les mêmes conditions commerciales (par exemple, le point d'expédition FAB) avec ses nouveaux clients américains. Lors de l'inspection de certains accords principaux avec ces nouveaux clients américains, vous constatez que la plus grande partie des conditions commerciales sont FAB à destination de livraison. Par conséquent, vous pouvez identifier un risque d'anomalies significatives lié à la survenance ou à la suppression de recettes, ou estimer que le risque inhérent est plus élevé que lorsque vous avez uniquement tenu compte des demandes d'informations comme fondement de votre évaluation des risques.

Compréhension du système de contrôle interne, y compris la composante « activités de contrôle »

À titre d'exemple, en réponse à vos demandes d'informations, le propriétaire peut déclarer que rien n'a changé en ce qui concerne la nature et l'étendue des processus et procédures utilisés pour garantir l'exactitude et l'exhaustivité de l'information financière. Cependant, les observations et l'inspection des rapports peuvent indiquer que le propriétaire n'a pas accédé aux rapports du système informatique de l'entité et ne les a pas contrôlés, alors qu'il a déclaré qu'il les examinait tous les mois. Une conversation de suivi avec le propriétaire peut permettre de corroborer les problèmes constatés lors de vos observations. De ce fait, vous pourriez évaluer le risque d'anomalies significatives comme étant plus élevé que si vous n'aviez pris en compte que les demandes d'informations comme fondement de votre évaluation des risques.

Conception et mise en œuvre des contrôles

L'évaluation de la conception d'un contrôle identifié consiste à examiner si le contrôle, seul ou en combinaison avec d'autres, a la capacité de prévenir, ou de détecter et corriger efficacement les anomalies significatives. La mise en œuvre d'un contrôle est déterminée par l'établissement de son existence et de son utilisation par l'entité. Cela ne peut pas être réalisé par la seule demande d'informations. Des procédures supplémentaires, notamment l'observation de l'application du contrôle pendant son exécution ou l'inspection de documents et de rapports, peuvent permettre de corroborer l'enquête sur la mise en œuvre du contrôle ou de fournir de nouvelles informations susceptibles influencer l'évaluation des risques et la réponse correspondante.

Par exemple, le propriétaire pourrait avoir recours à certains rapports informatiques pour réaliser un contrôle concernant un risque substantiel. Vous pouvez poser des questions afin de comprendre comment les rapports sont générés ainsi que la nature, le calendrier et l'étendue de leur utilisation. Cependant, il se peut que vous soyez incapable de déterminer si le propriétaire du contrôle génère ou utiliser le rapport d'une manière différente que celle qui vous a été expliquée sans observer le processus de génération et d'utilisation des rapports concernés. En conséquence, vous pourriez être amené à reconsidérer votre identification des risques éventuels d'anomalies significatives, ou à concevoir des procédures supplémentaires ou différentes sur l'utilisation de ces rapports pour la collecte d'éléments probants, et à déterminer si cela constitue une déficience en vertu de la norme ISA 265.

Les politiques et procédures (et contrôles) de l'entité peuvent être imposées par des documents officiels ou par d'autres communications de la direction ou de responsables de la gouvernance, ou être le résultat de comportements qui, sans être imposés, sont conditionnés par la culture de l'entité. Dans les entités peu complexes, il se peut que les éléments probants concernant les éléments de l'environnement de contrôle ne soient pas disponibles sous forme de documents, en particulier là où les communications entre la direction et le personnel sont informelles, mais qu'ils soient tout de même suffisamment pertinents et fiables dans les circonstances. Vous pourriez envisager d'observer l'application de contrôles particuliers et de parler avec plusieurs personnes de l'entité afin de corroborer vos enquêtes initiales.

O3 – Pourquoi devez-vous acquérir une compréhension de chacune des cinq composantes de contrôle interne même si votre approche de l'audit est essentiellement à des fins de corroboration ?

(Norme ISA 315.21-27)

Vous êtes tenu d'acquérir cette compréhension afin de pouvoir identifier et évaluer les risques d'anomalies significatives au niveau des états financiers et au niveau des assertions. Si vous ne disposez pas d'une telle compréhension, vous pourriez, par exemple, manquer

- d'identifier un risque d'anomalie significative,
- d'évaluer de façon appropriée le risque identifié d'anomalies significatives, ou
- de répondre de façon appropriée à un risque identifié lors de la conception et de la mise en œuvre de vos procédures d'audit complémentaires.

Retour à la **Figure 1**.

(Remarque : pour consulter les exigences de la norme ISA 315 (révisée en 2019) liées à l'acquisition de la compréhension du système de contrôle interne de l'entité au format en diagramme, se reporter à l'**Annexe A** du présent *outil*).

La norme ISA 315 (révisée en 2019) fournit des informations sur la « manière » d'acquérir une compréhension des cinq composantes du contrôle interne. Cela se fait par :

- une compréhension d'éléments spécifiques au sein d'une composante de contrôle interne ; et
- une évaluation pour déterminer si les contrôles de cette composante de contrôle interne sont appropriés à la nature et aux circonstances de l'entité.

En vous fondant sur les résultats de l'évaluation de la pertinence des contrôles pour cette entité (c'est-à-dire, votre évaluation de chacune des composantes du système de contrôle interne de l'entité), vous devez déterminer si une ou plusieurs déficiences de contrôle ont été identifiées. Si vous avez identifié une ou plusieurs déficiences de contrôle, vous pouvez prendre en considération l'incidence de ces déficiences sur les procédures d'audit complémentaires à concevoir conformément à la norme ISA 330.

La norme ISA 315 (révisée en 2019) reconnait que la conception, la mise en œuvre et la maintenance du système de contrôles internes d'une entité varient en fonction de sa taille et de sa complexité. Par exemple, les entités peu complexes peuvent utiliser des contrôles plus simples ou moins structurés (par exemple, des politiques et des procédures) afin d'atteindre leurs objectifs[27]. Ces contrôles plus simples peuvent être appropriés aux circonstances des entités peu complexes.

En plus de fournir des informations sur la « manière » d'acquérir une compréhension des cinq composantes du contrôle interne, la norme ISA 315 (révisée en 2019) fournit également des informations sur la « raison » pour laquelle vous devez acquérir une compréhension de chacune des composantes du système de contrôle interne d'une entité, dans le cadre de la préparation des états financiers du matériel d'application.

Un bref aperçu des raisons pour lesquelles il est nécessaire d'acquérir une compréhension de chacun des éléments est présenté ci-dessous, dans le contexte de l'audit d'une entité peu complexe. Des questions particulières pouvant nécessiter des clarifications sont indiquées avec des suggestions sur la façon de les aborder.

Environnement de contrôle

Vous devez acquérir une compréhension de l'environnement de contrôle de l'entité peu complexe, car celui-ci (par exemple, donner le ton au sommet) peut avoir une incidence sur les risques d'anomalies significatives (y compris les risques de fraude) au niveau des états financiers, ce qui affecterait à son tour les risques d'anomalies significatives au niveau des assertions.

27 Norme ISA 315.A92.

Cela est dû au fait que l'environnement de contrôle fournit une base générale pour les opérations des autres composantes du système de contrôle interne[28]. Il peut avoir une influence considérable sur l'efficacité des contrôles dans les autres composantes et sur la préparation des états financiers. Par exemple, si le propriétaire d'une entreprise donne le ton au sommet en soulignant l'importance de l'honnêteté et de l'intégrité, en accordant une grande priorité aux contrôles et en exigeant le respect des politiques et procédures établies, cela peut contribuer au fonctionnement efficace des contrôles de l'entité afin de détecter et de corriger toute anomalie et, par conséquent, de réduire la possibilité des risques d'anomalies significatives. Par ailleurs, même les politiques informelles d'une entité peu complexe en matière de ressources humaines (par exemple, les politiques et procédures relatives à l'embauche d'employés compétents et expérimentés) sont susceptibles de constituer un facteur déterminant quant aux caractéristiques du personnel nécessaire pour garantir la qualité de l'information financière. Vous devez utiliser cette compréhension pour évaluer si la direction a créé et maintenu une culture d'honnêteté et de comportement éthique, et si l'environnement de contrôle constitue une base appropriée pour les autres composantes du système de contrôle interne de l'entité.

Des informations probantes relatives à la qualité de l'environnement de contrôle peuvent être obtenues en interrogeant le propriétaire sur les différents aspects de l'exercice de son rôle (c'est-à-dire les responsabilités et la culture en matière de supervision) et en observant, tout au long de l'audit, les activités de la direction générale et ses interactions avec le reste du personnel. En outre, en procédant à des enquêtes auprès d'autres membres du personnel, vous pouvez obtenir des points de vue différents sur la qualité de l'environnement de contrôle nécessaire à la compréhension. Lors de l'évaluation de l'environnement de contrôle, il convient de tenir compte des informations obtenues lors de la compréhension de l'environnement de contrôle afin de déterminer si celui-ci est adapté à la nature et aux circonstances de l'entité ou s'il existe une déficience. Il faut noter qu'il s'agit d'une évaluation de l'environnement de contrôle dans son ensemble et de la manière dont il soutient les autres composantes du système de contrôle interne de l'entité, et non d'une évaluation détaillée de contrôles spécifiques au sein de l'environnement de contrôle (le cas échéant).

Processus d'évaluation des risques de l'entité

Comme toutes les entités, une entité peu complexe est confrontée à des risques d'entreprise. Ceux-ci découlent, par exemple, de conditions et événements importants qui peuvent avoir une incidence négative sur l'atteinte des objectifs de l'entité peu complexe. Le propriétaire (et parfois le conseil d'administration) disposera d'un processus, probablement informel, visant à identifier, à évaluer et à gérer les risques d'entreprise. Votre compréhension de ce processus vous permettra de savoir où l'entité identifie ses risques et si l'entité peu complexe a fait face à ces risques, et d'évaluer si son processus d'évaluation des risques est approprié aux circonstances, compte tenu de la nature et de la complexité de l'entité peu complexe.

Par exemple, si l'entité peu complexe est un fabricant, il existe un risque de détérioration de la qualité des produits. Si la direction de l'entité peu complexe ne gère pas ce risque de quelque façon que ce soit, les effets sur les états financiers peuvent inclure, par exemple, des problèmes d'évaluation des stocks, des problèmes accrus de recouvrement des comptes ayant une incidence sur la provision pour créances douteuses et une nécessité de revoir à la hausse les estimations relatives aux garanties. En vous fondant sur cette compréhension, vous pouvez, lors de l'évaluation du processus d'évaluation des risques de l'entité, identifier une déficience de contrôle et tenir compte de son incidence sur l'audit.

De même, l'évaluation des risques d'entreprise de l'entité peu complexe par la direction aura une incidence sur son appréciation de la capacité de l'entité à poursuivre ses activités.

Même si les éléments probants de l'évaluation des risques ne sont pas formellement documentés, les demandes d'informations adressées au propriétaire et à d'autres employés compétents vous permettront de comprendre comment et à quelle fréquence les risques d'entreprise sont pris en compte. Lors de l'évaluation du processus d'évaluation des risques de l'entité, il convient de déterminer si les mesures prises par l'entité sont adaptées à sa nature et à ses circonstances ou s'il existe une déficience (par exemple, pour les entités plus petites et moins complexes, il peut être approprié dans certains cas de ne pas disposer d'un processus formel pour l'évaluation des risques).

28 Norme ISA 315.A97.

Processus de suivi du système de contrôle interne de l'entité

Vous devez comprendre cette composante, à savoir si, comment et quand le suivi de l'entité est effectué, car celui-ci aura une incidence, par exemple, sur la prévention ou la détection d'anomalies (significatives ou non).

Une entité peu complexe peut ne pas disposer d'un processus formel pour le suivi de son système de contrôle interne. Cependant, les risques d'inexactitude de l'information financière peuvent être plus faibles, par exemple, lorsque le propriétaire est activement impliqué dans le suivi de certains aspects des opérations, comme le recouvrement des créances, le règlement ponctuel des fournisseurs et le respect des clauses contractuelles des prêts. À cet effet, le propriétaire pourrait avoir recours aux rapports générés par un logiciel commercial.

Pour mieux comprendre le processus de suivi, il est probable qu'il soit nécessaire de mener des enquêtes auprès du propriétaire ou d'autres membres du personnel impliqués dans ce processus. Vous pouvez observer ou inspecter la documentation qui indique la nature et la fréquence des activités de suivi. Cette compréhension vous permettra d'évaluer si le processus de suivi du système de contrôle interne par l'entité est approprié aux circonstances de l'entité, compte tenu de la nature et de la complexité de celle-ci (par exemple, l'entité n'effectue pas de suivi mais, même dans les entités peu complexes plus petites, un certain suivi serait attendu, car une déficience pourrait exister).

Système d'information et communications

(Remarque : pour consulter les exigences de la norme ISA 315 (révisée en 2019) liées à l'acquisition par l'auditeur d'une compréhension du système de l'environnement informatique et de l'identification des contrôles généraux informatiques au format en diagramme, se reporter à l'**Annexe B** du présent *outil*). Voir la question **O4** pour une discussion sur les questions de contrôle interne lors de l'utilisation par l'entité peu complexe d'un logiciel commercial).

Système d'information relatif à la préparation des états financiers

Vous devez acquérir une compréhension du système d'information, car il est possible que des anomalies résultent d'événements survenant à n'importe quel point du flux d'informations relatif à l'information financière. Par conséquent, vous devez tenir compte des éléments suivants lors de l'acquisition de la compréhension :

- les politiques du système d'information relatives à la nature des données ou des informations liées aux transactions ;
- les autres événements et conditions à prendre en compte ;
- le traitement de l'information visant à maintenir l'intégrité des données ou de l'information en question ;
- les processus d'information, le personnel et les autres ressources utilisés dans le traitement de l'information.

Cela englobe les informations provenant non seulement du grand livre et des livres auxiliaires, mais également d'autres sources, telles que les feuilles de calcul utilisées pour calculer les produits comptabilisés ou externes à l'entité (comme les taux d'intérêt) lorsqu'elles sont utilisées, par exemple, dans le calcul de la juste valeur.

Bien que les systèmes d'information des entités peu complexes ne soient pas forcément complexes, il existe cependant des risques d'anomalies significatives, par exemple si les membres du personnel ne disposent pas des compétences ou des autres ressources nécessaires à l'accomplissement de leurs tâches ou si la séparation des tâches n'est pas correctement assurée. En vous fondant sur cette compréhension, vous pouvez, lors de l'évaluation du système d'information de l'entité, identifier une déficience de contrôle et tenir compte de son incidence sur l'audit.

Une entité peu complexe peut ne pas disposer de manuels de politiques et de procédures ou de documentation formelle sur le système d'information (bien qu'il s'agisse d'une bonne pratique, même dans les petites organisations). Là encore, la recherche et l'observation (par exemple en effectuant une visite) du déroulement des différents processus pertinents peuvent vous permettre de comprendre le système d'information. Cela implique la prise en compte de l'environnement informatique de l'entité (par exemple, la manière d'utiliser le logiciel commercial pour traiter l'information).

Les auditeurs peuvent parfois confondre la composante « système d'information » du contrôle interne avec la composante « activités de contrôle ». Comme décrit ci-dessous dans la section « activités de contrôle », ces composantes sont différentes (mais interdépendantes) ; mais il est important de savoir les différencier. Les contrôles de la composante « activités de contrôle » sont identifiés dans le cadre du travail effectué pour comprendre l'ensemble du système d'information.

Communications relatives à la préparation des états financiers

Vous devez acquérir une compréhension du système d'information, car cela peut avoir une incidence, par exemple, sur l'exactitude et l'exhaustivité de l'information financière.

Les communications au sein d'une entité peu complexe peuvent être informelles. Néanmoins, le risque d'obtenir une information financière inexacte peut être moindre, par exemple, si les questions liées à l'information financière, notamment les rôles et les responsabilités, sont communiquées de manière claire et en temps utile. Les communications adressées par le propriétaire au personnel concerné sur les décisions de l'entreprise, telles que la modification de la politique d'octroi de crédits aux clients, peuvent également compromettre l'exactitude de la comptabilité. Dans un autre exemple, le propriétaire peut être au courant d'accords parallèles avec des clients ou des fournisseurs, sans pour autant avoir communiqué cette information au personnel de la comptabilité. Cela peut se traduire par une comptabilisation inexacte des charges à payer.

En outre, une communication en temps utile adressée par les autres membres du personnel au propriétaire sur les problèmes comptables identifiés ou sur les changements de circonstances susceptibles d'affecter leur capacité à s'acquitter de leurs responsabilités peuvent également contribuer à réduire le risque d'inexactitude de l'information financière.

Des demandes d'informations sur les processus de communication, l'observation de ces processus et l'examen de la documentation pertinente, le cas échéant, pourraient vous permettre de comprendre le processus de communication. Cette compréhension vous permettra de déterminer sur la communication mise en œuvre au sein de l'entité soutient de manière appropriée la préparation des états financiers de l'entité conformément au référentiel d'information financière applicable.

Activités de contrôle

Vous devez acquérir une compréhension de la composante « activités de contrôle » parce que les contrôles qu'elle comprend sont conçus pour garantir la bonne application des politiques (qui sont des contrôles) dans toutes les autres composantes du système de contrôle interne de l'entité[29]. Les contrôles de la composante « activités de contrôle » peuvent donc se révéler particulièrement importants dans la gestion des risques d'anomalies significatives.

Distinction entre la composante « systèmes d'information » et la composante « activités de contrôle »

Les exigences relatives à la composante « systèmes d'information » sont destinées à vous fournir une base pour comprendre le cheminement de l'information à travers le système d'information, les registres comptables, le processus d'information financière utilisé pour préparer les états financiers et les informations à fournir, ainsi que les ressources de l'entité, notamment l'environnement informatique. La composante « activités de contrôle » comporte des contrôles tels que les autorisations et les approbations, les rapprochements, les vérifications, les contrôles physiques ou logiques (y compris les contrôles d'accès aux programmes informatiques et aux fichiers de données) et la séparation des tâches. Pour la composante « activités de contrôle », vous devez évaluer la conception et déterminer la mise en œuvre des contrôles spécifiques identifiés qui répondent aux exigences. Cette exigence s'applique même si vos procédures pour répondre aux risques évalués sont essentiellement corroboratives. Il ne vous incombe pas d'évaluer la conception et de déterminer la mise en œuvre de tous les contrôles de la composante « systèmes d'information et de communication », mais vous devez évaluer si les systèmes d'information et de communication de l'entité soutiennent de manière appropriée la préparation des états financiers (voir la question **N1**).

29 Norme ISA 315.A147.

O4 – Comment votre approche de l'identification, de l'évaluation de la conception et de la détermination de la mise en œuvre des contrôles généraux informatiques (CGI) peut-elle tenir compte du fait qu'une entité peu complexe utilise un logiciel commercial non complexe pour la comptabilité et l'information financière ?

(ISA 315.26(b)-(c) ; A170 ; Annexe 5 et Annexe 6)

Lorsqu'une entité peu complexe utilise des logiciels commerciaux, vos procédures d'évaluation des risques concernant les contrôles généraux informatiques peuvent nécessiter moins d'efforts que pour l'audit d'une entité disposant d'un environnement informatique sophistiqué. Les procédures relatives à la conception et à la mise en œuvre des contrôles généraux informatiques peuvent être axées sur la gestion de l'accès au système par rapport aux contrôles de gestion des changements ou aux contrôles opérationnels informatiques.

(Voir la question **N5** – les contrôles généraux informatiques sont parmi les contrôles de la composante « activités de contrôle » spécifiés dans la norme ISA 315.26.)

Retour à la **Figure 1**.

D'une manière générale, les aspects suivants de l'informatique doivent être abordés pour comprendre le système d'information :

- l'environnement informatique relatif au système d'information (nouvellement défini (se reporter à la nouvelle définition ci-dessus)). Les paragraphes A140–A141 de la norme ISA 315 (révisée en 2019) expliquent « pourquoi » cette compréhension est nécessaire ; et
- l'utilisation de l'informatique par l'entité (c'est-à-dire les applications informatiques relatives aux flux de transactions et au traitement de l'information dans le système d'information). Les paragraphes A142–A143 de la norme ISA 315 (révisée en 2019) fournissent des explications supplémentaires sur la compréhension acquise par l'auditeur sur le recours à l'informatique lors de la compréhension du système d'information.

Selon le paragraphe 26(b) de la norme ISA 315 (révisée en 2019), l'auditeur ne doit identifier que les applications informatiques et les autres aspects de l'environnement informatique qui présentent des risques découlant du recours à l'informatique. Certaines entités peu complexes utilisent un logiciel comptable commercial « prêt à l'emploi » dont le code source ne peut pas être modifié par l'entité. Par conséquent, les risques informatiques liés à la préparation des états financiers de l'entité seront probablement très limités. Il est également possible que les contrôles généraux informatiques des entités peu complexes puissent ne pas être formels[30].

La norme ISA 315 (révisée en 2019) admet que l'étendue de la compréhension par l'auditeur des processus informatiques, y compris la mesure dans laquelle l'entité a mis en place des contrôles généraux informatiques, dépendra de la nature et des circonstances de l'entité et de son environnement informatique. Il faut également préciser que la norme ISA 315 (révisée en 2019) contient des indications beaucoup plus détaillées sur les questions dont il faut tenir compte pour acquérir une compréhension de l'environnement et des contrôles informatiques d'une entité.

Par exemple, l'annexe 5 fournit des exemples des caractéristiques types des environnements informatiques en fonction de la complexité des applications informatiques utilisées dans le système d'information de l'entité. Cela comprend un tableau de comparaison des caractéristiques types des éléments suivants :

- Logiciel commercial peu complexe
- Logiciel commercial ou applications informatiques de moyenne envergure et modérément complexes
- Applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés)

30 Norme ISA 315.A241.

De même, l'Annexe 6 de la norme ISA 315 (révisée en 2019) comprend un tableau d'exemples illustrant les contrôles généraux informatiques pour gérer les risques d'utilisation de l'informatique dans différentes applications informatiques pour les logiciels commerciaux des trois niveaux de complexité. Par exemple, vous pouvez identifier certains contrôles automatisés liés au logiciel commercial unique et non complexe d'une entité peu complexe pour la préparation des rapports financiers, qui contient des rapports standard générés par le logiciel. L'entité peu complexe n'a pas la possibilité de modifier le programme, car elle ne possède pas le code source. L'infrastructure informatique prenant en charge l'application informatique se rapporte à un seul réseau, un seul système d'exploitation et une seule base de données. Les opérations informatiques n'impliquent pas la sauvegarde des données, car les sauvegardes manuelles sont réalisées par l'équipe financière et il n'y a pas d'opérations de planification des tâches. Par conséquent, vous identifiez les processus liés à l'accès (et non au changement ou aux opérations informatiques) comme étant exposés aux risques découlant du recours à l'informatique. Vous devez identifier les risques suivants découlant du recours à l'informatique et aux contrôles généraux informatiques qui mitigent ces risques :

Processus informatique	Exemple de risques découlant du recours à l'informatique	Exemples de contrôles généraux informatiques
Gestion de l'accès	Privilèges d'accès utilisateur : Utilisateurs détenant des privilèges d'accès supérieurs à ceux qui sont nécessaires pour l'exercice de leurs fonctions, ce qui peut entraîner une mauvaise séparation des tâches.	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.
		L'accès des utilisateurs résiliés ou transférés est supprimé ou modifié en temps opportun.
		L'accès utilisateur est soumis à des revues périodiques.
		L'accès privilégié (par exemple, les droits d'administrateurs permettant de gérer la configuration, les données et la sécurité) est dûment autorisé et strictement limité.
	Configuration des systèmes : Systèmes qui, faute d'être configurés ou mis à jour de façon adéquate, ne permettent pas de restreindre l'accès aux seuls utilisateurs appropriés et dûment autorisés.	Pour accéder aux systèmes, les utilisateurs doivent s'authentifier au moyen de codes d'utilisateur et de mots de passe uniques ou d'autres mécanismes de validation des droits d'accès. Les paramètres des mots de passe répondent aux normes de l'entreprise ou du secteur (longueur minimale et niveau de complexité exigés, expiration du mot de passe, verrouillage du compte, etc.).

Même dans le cas d'un audit d'une entité peu complexe, votre évaluation du système d'information de l'entité peut inclure, par exemple, une analyse visant à déterminer si l'entité a investi dans un environnement informatique approprié et dans les améliorations nécessaires. Vous pouvez également vérifier si l'entité a employé un nombre suffisant de personnes dûment qualifiées lors de l'utilisation de logiciels commerciaux (même si la possibilité de les modifier est nulle ou limitée).

Un autre facteur à prendre en compte est que les contrôles que vous identifiez peuvent dépendre de rapports générés par le système. Les applications informatiques qui produisent ces rapports peuvent être vulnérables aux risques découlant du recours à l'informatique. Lorsque vous abordez votre audit dans le cadre d'une approche de corroboration, vous pouvez décider de tester directement les données d'entrée et de sortie du processus de génération de rapports. Dans ce cas, il se peut que vous n'identifiiez pas les applications informatiques connexes comme étant soumises aux risques découlant du recours à l'informatique[31]. Par conséquent, les contrôles appliqués à ces rapports générés par le système (qui font partie de la composante « activités de contrôle ») peuvent ne pas avoir besoin d'une évaluation dans le cadre de votre processus d'évaluation des risques.

31 Norme ISA 315.A169.

O5 – La nature et l'étendue de votre documentation peuvent-elles prendre en compte le fait que l'entité et ses processus sont moins complexes en ce qui concerne l'audit d'une entité peu complexe ? (Norme ISA 315.38)

Dans le cas des audits d'états financiers des entités peu complexes, la forme et l'étendue de la documentation peuvent être simples et relativement succinctes. Toutefois, votre documentation doit être suffisante pour permettre à un auditeur expérimenté, n'ayant aucun lien antérieur avec l'audit, de comprendre, par exemple, la nature, le calendrier et l'étendue des procédures d'évaluation des risques que vous avez mises en œuvre pour vous conformer à la norme ISA 315 (révisée en 2019), ainsi que les résultats de ces procédures.

Retour à la **Figure 1**.

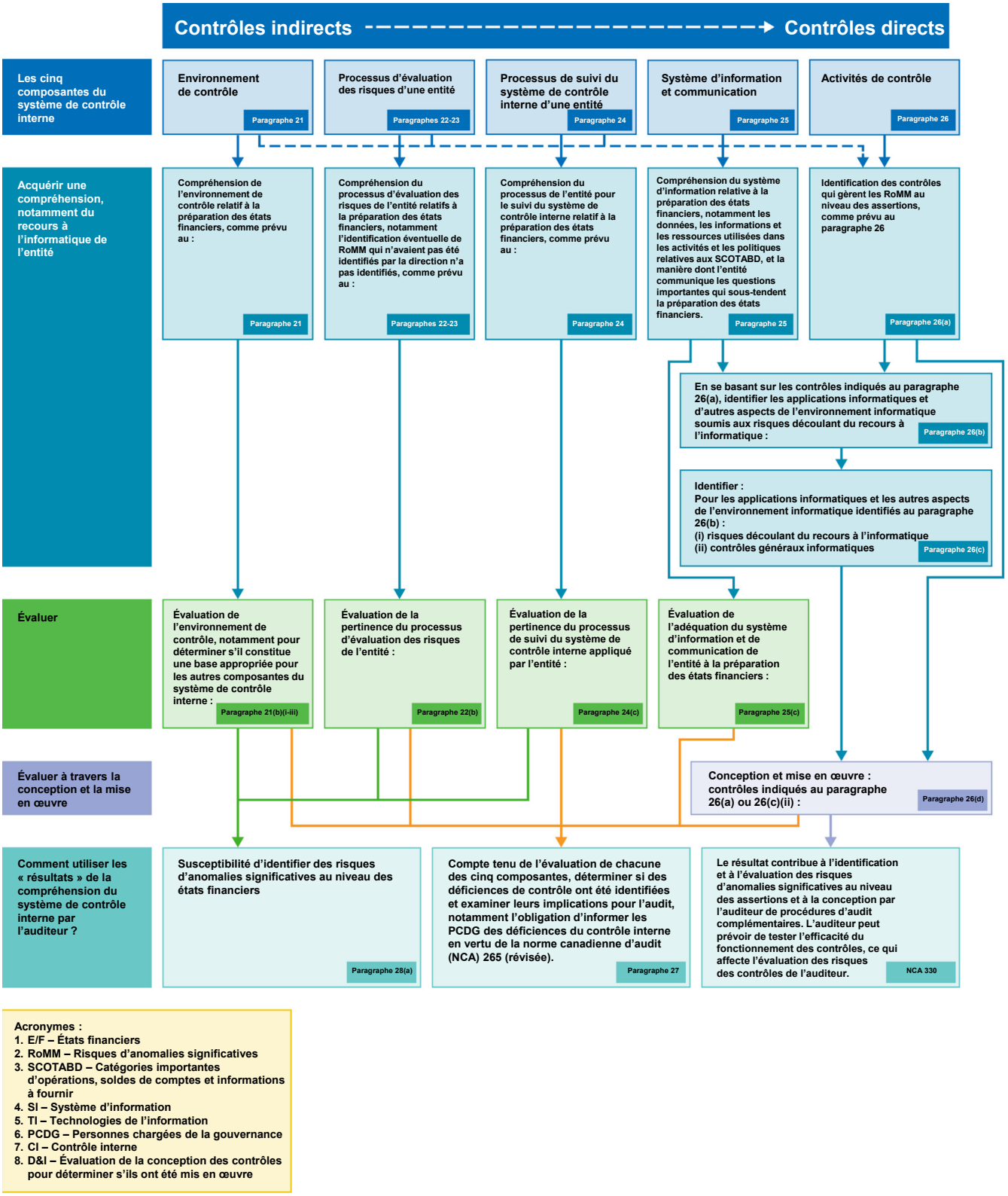
Certains auditeurs ont estimé que la nature et le niveau de précision de la documentation requise pour l'identification et l'évaluation des risques manquent de clarté.

L'étendue de la documentation est laissée à la discrétion de l'auditeur ; ces normes sont fondées sur des principes. La norme ISA 315 (révisée en 2019) indique que votre documentation est influencée, par exemple, par la nature, la taille et la complexité de l'entité et de son système de contrôle interne, par la disponibilité des informations fournies par l'entité, ainsi que par la méthodologie et la technologie d'audit employées au cours de l'audit. Il n'est pas nécessaire de documenter l'intégralité de votre compréhension de l'entité et des questions qui s'y rapportent[32]. La documentation des éléments clés de la compréhension peut inclure ceux sur lesquels vous vous êtes fondé pour évaluer les risques d'anomalies significatives. Toutefois, vous n'êtes pas tenu de documenter chaque facteur de risque inhérent que vous avez pris en compte lors de l'identification et l'évaluation des risques d'anomalies significatives au niveau des assertions (comme expliqué dans la question **N3**). Dans les audits des entités peu complexes, la documentation de l'audit peut être intégrée dans la documentation de l'auditeur à la stratégie globale et au plan d'audit.

32 Norme ISA 315.A241.

Annexe A

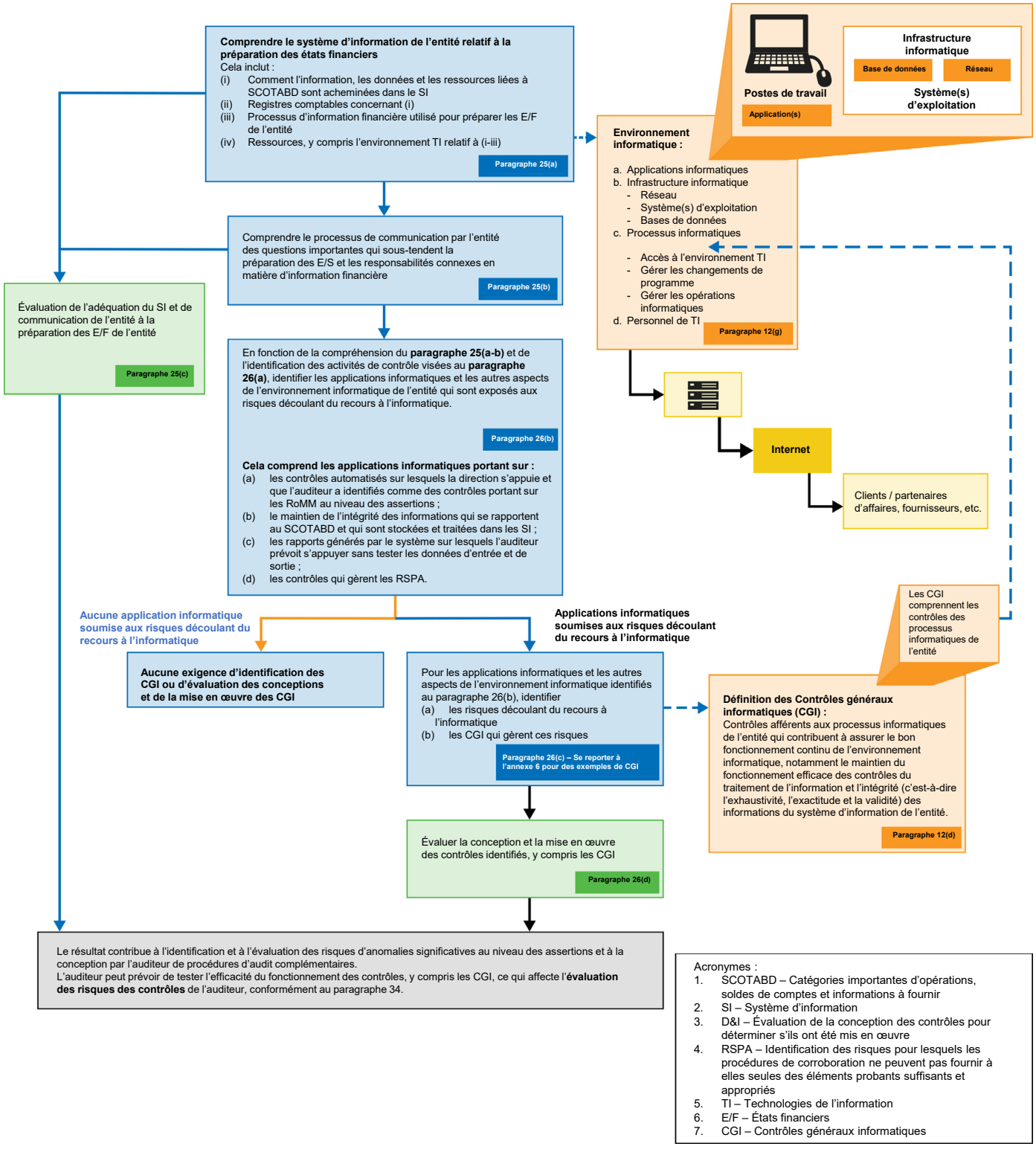
Compréhension des composantes du système de contrôle interne de l'entité[33]



33 Cette figure est extraite du document *Compréhension de l'organigramme du contrôle interne* du Conseil international des normes d'audit et d'assurance, publié par la Fédération internationale des experts-comptables en juillet 2018.

Annexe B

Compréhension du recours de l'entité à l'informatique[34]



34 Cette figure est extraite du document *Compréhension de l'organigramme de l'environnement informatique* du Conseil international des normes d'audit et d'assurance, publié par la Fédération internationale des experts-comptables en juillet 2018.

Pour en savoir plus, veuillez contacter ChristopherArnold@ifac.org.

International Federation of Accountants®

529 Fifth Avenue, 6e étage
New York, NY 10017
www.ifac.org