

Prise de position définitive
Décembre 2019

ISA™

Norme internationale d'audit 315 (révisée 2019)

Norme ISA 315 (révisée 2019)

*Identification et évaluation des
risques d'anomalies significatives*

et

*modifications de concordance
et modifications corrélatives
apportées à d'autres
normes internationales par suite de la
publication de la norme ISA 315
(révisée 2019)*

Élaborée par :



International Auditing
and Assurance
Standards Board™

Traduite par :



COMPTABLES
PROFESSIONNELS
AGRÉÉS
CANADA

À propos de l'IAASB

Le présent document a été élaboré et approuvé par le Conseil des normes internationales d'audit et d'assurance (*International Auditing and Assurance Standards Board, IAASB*).

L'IAASB a pour objectif de servir l'intérêt public en établissant des normes d'audit et d'assurance et d'autres normes connexes de haute qualité, de même qu'en facilitant la convergence des normes d'audit et d'assurance internationales et nationales, rehaussant ainsi la qualité et la constance de la pratique et renforçant la confiance du public à l'égard de la profession mondiale d'audit et d'assurance.

L'IAASB élabore des normes d'audit et d'assurance ainsi que des lignes directrices applicables par l'ensemble des professionnels comptables par le truchement d'un processus partagé d'établissement des normes auquel participent le Conseil de supervision de l'intérêt public (*Public Interest Oversight Board*), qui supervise les activités de l'IAASB, et le Groupe consultatif (*Consultative Advisory Group*) de l'IAASB, qui recueille les commentaires du public aux fins de l'élaboration des normes et des lignes directrices. L'IAASB dispose des structures et des processus nécessaires à l'exercice de ses activités grâce au concours de l'*International Federation of Accountants* (IFAC).

Copyright © 2019 International Federation of Accountants (IFAC). Pour obtenir des renseignements sur les droits d'auteur, les marques de commerce et les permissions, veuillez consulter la page 200.

SOMMAIRE

	Page
Norme ISA 315 (révisée 2019), <i>Identification et évaluation des risques d'anomalies significatives</i>	4
Modifications de concordance et modifications corrélatives apportées à d'autres normes internationales	129

NORME INTERNATIONALE D'AUDIT (ISA) 315 (RÉVISÉE 2019)

IDENTIFICATION ET ÉVALUATION DES RISQUES D'ANOMALIES SIGNIFICATIVES

(Applicable aux audits d'états financiers pour les périodes ouvertes à compter du 15 décembre 2021)

SOMMAIRE

	Paragraphe
Introduction	
Champ d'application de la présente norme ISA	1
Concepts fondamentaux de la présente norme ISA	2
Application proportionnée	9
Date d'entrée en vigueur	10
Objectif	11
Définitions	12
Diligences requises	
Procédures d'évaluation des risques et activités connexes	13–18
Prise de connaissance de l'entité et de son environnement, du référentiel d'information financière applicable et du système de contrôle interne de l'entité	19–27
Identification et évaluation des risques d'anomalies significatives	28–37
Documentation	38
Modalités d'application et autres commentaires explicatifs	
Définitions.....	A1–A10
Procédures d'évaluation des risques et activités connexes	A11–A47
Prise de connaissance de l'entité et de son environnement, du référentiel d'information financière applicable et du système de contrôle interne de l'entité	A48–A183
Identification et évaluation des risques d'anomalies significatives	A184–A236
Documentation	A237–A241
Annexe 1 : Éléments à prendre en considération pour prendre connaissance de l'entité et de son modèle économique	
Annexe 2 : Connaissance des facteurs de risque inhérent	
Annexe 3 : Connaissance du système de contrôle interne de l'entité	
Annexe 4 : Éléments à prendre en considération pour prendre connaissance de la fonction d'audit interne de l'entité	
Annexe 5 : Éléments à prendre en considération pour prendre connaissance du recours à l'informatique par l'entité	

Annexe 6 : Éléments à prendre en considération pour prendre connaissance des contrôles généraux informatiques

La Norme internationale d'audit (ISA) 315 (révisée en 2019), *Identification et évaluation des risques d'anomalies significatives*, doit être lue conjointement avec la norme ISA 200, *Objectifs généraux de l'auditeur indépendant et conduite d'un audit selon les Normes internationales d'audit*.

La norme ISA 315 (révisée en 2019) a été approuvée par le Conseil de supervision de l'intérêt public (PIOB), qui a conclu qu'elle a été élaborée dans le respect de la procédure officielle et que l'intérêt public a dûment été pris en compte.

Introduction

Champ d'application de la présente norme ISA

1. La présente Norme internationale d'audit (ISA) traite des obligations de l'auditeur concernant l'identification et l'évaluation des risques d'anomalies significatives contenues dans les états financiers.

Concepts clés de la présente norme ISA

2. La norme ISA 200 traite des objectifs généraux de l'auditeur lors de la conduite d'un audit d'états financiers¹, dont celui qui consiste à recueillir des éléments probants suffisants et appropriés pour réduire le risque d'audit à un niveau suffisamment faible². Le risque d'audit est fonction des risques d'anomalies significatives et du risque de non-détection³. La norme ISA 200 précise que les risques d'anomalies significatives peuvent se situer à deux niveaux⁴ : au niveau des états financiers pris dans leur ensemble ; et au niveau des assertions pour des flux d'opérations, des soldes de comptes ou des informations fournies dans les états financiers.
3. La norme ISA 200 requiert que l'auditeur exerce son jugement professionnel lors de la planification et de la réalisation d'un audit et qu'il fasse preuve d'esprit critique tout au long de la planification et de la réalisation de l'audit, en étant conscient qu'il peut exister des situations conduisant à ce que les états financiers comportent des anomalies significatives⁵.
4. Les risques au niveau des états financiers visent les risques d'anomalies significatives qui touchent de manière diffuse les états financiers pris dans leur ensemble et qui affectent potentiellement plusieurs assertions. Les risques d'anomalies significatives au niveau des assertions comportent deux composantes : le risque inhérent et le risque lié au contrôle interne :
 - le risque inhérent est défini comme la possibilité qu'une assertion portant sur un flux d'opérations, un solde de compte ou une information fournie dans les états financiers, comporte une anomalie qui pourrait être significative, individuellement ou cumulée avec d'autres, avant la prise en compte des contrôles y afférents un flux d'opérations ;
 - le risque lié au contrôle interne est défini comme le risque qu'une anomalie susceptible de se produire au niveau d'une assertion portant sur un flux d'opérations, un solde de compte ou une information fournie dans les états financiers et qui pourrait être significative individuellement ou cumulée avec d'autres, ne soit ni prévenue, ni détectée et corrigée en temps voulu par le contrôle interne de l'entité un flux d'opérations.
5. La norme ISA 200 explique que l'évaluation des risques d'anomalies significatives au niveau des assertions vise à permettre de déterminer la nature, le calendrier et l'étendue des procédures d'audit complémentaires nécessaires à l'obtention d'éléments probants suffisants et appropriés⁶. En ce qui concerne les risques d'anomalies significatives identifiés au niveau des assertions, la présente norme ISA requiert que le risque inhérent et le risque lié au contrôle interne soient évalués séparément.. Comme le précise la norme ISA 200, le risque inhérent est plus élevé pour certaines assertions et pour certains flux d'opérations, soldes de comptes ou informations à fournir les concernant que pour d'autres. La mesure dans laquelle le risque inhérent varie , est désignée dans la présente norme ISA, par l'expression « échelle de risque inhérent ».

¹ Norme ISA 200, *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux Normes internationales d'audit*.

² Norme ISA 200, paragraphe 17.

³ Norme ISA 200, paragraphe 13(c).

⁴ Norme ISA 200, paragraphe A36.

⁵ Norme ISA 200, paragraphes 15–16.

⁶ Norme ISA 200, paragraphe A43(a) et norme ISA 330, *Réponses de l'auditeur à l'évaluation des risques*, paragraphe 6.

6. L'auditeur identifie et évalue les risques d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs. Les unes et les autres sont traités dans la présente norme ISA ; toutefois, l'importance de la fraude est telle que des diligences et des modalités d'application supplémentaires sont fournies dans la norme ISA 240⁷ en relation avec les procédures d'évaluation des risques et des procédures liées, afin de recueillir des informations qui sont utilisées pour identifier, évaluer et répondre aux risques d'anomalies significatives résultant de fraudes.
7. Le processus d'identification et d'évaluation des risques par l'auditeur est itératif et dynamique. Il existe une relation d'interdépendance entre, d'une part, la connaissance de l'entité et de son environnement, du référentiel comptable applicable ainsi que du système de contrôle interne que doit acquérir l'auditeur et, d'autre part, les concepts qui sous-tendent les diligences d'identification et d'évaluation des risques d'anomalies significatives. Pour acquérir la connaissance exigée par la présente norme ISA, l'auditeur peut établir des attentes initiales concernant les risques – attentes qu'il affinera à mesure qu'il progresse dans le processus d'identification et d'évaluation des risques. Par ailleurs, la présente norme ISA et la norme ISA 330 requièrent que l'auditeur réévalue son évaluation des risques et modifie l'approche générale et les procédures d'audit complémentaires en fonction des éléments probants recueillis lors de la mise en œuvre, conformément à la norme ISA 330, des procédures d'audit complémentaires, et de toute information nouvelle dont il prend connaissance.
8. La norme ISA 330 requiert que l'auditeur conçoive et mette en œuvre une approche générale pour répondre aux risques d'anomalies significatives au niveau des états financiers⁸. Elle précise que l'évaluation par l'auditeur des risques d'anomalies significatives au niveau des états financiers et, par voie de conséquence, l'approche générale à retenir, sont influencées par la connaissance qu'a l'auditeur de l'environnement de contrôle. La norme ISA 330 requiert aussi que l'auditeur conçoive et mette en œuvre des procédures d'audit complémentaires dont la nature, le calendrier et l'étendue sont fonction des risques évalués d'anomalies significatives au niveau des assertions et y répondent⁹.

Application proportionnée

9. Dans la norme ISA 200, il est précisé que certaines normes ISA comportent des considérations relatives à l'application proportionnée dont le but est d'illustrer l'application des diligences à toutes les entités, que leur nature et leurs circonstances soient peu complexes ou très complexes¹⁰. La présente norme ISA vise les audits de toutes les entités, peu importe leur taille ou leur complexité. On y trouve donc, dans les modalités d'application, des considérations propres aux entités peu complexes et aux entités plus complexes, lorsque cela est pertinent. S'il est vrai que la taille de l'entité peut être un indicateur de sa complexité, il existe tout de même de petites entités qui sont complexes et, à l'inverse, de grandes entités qui sont peu complexes.

Date d'entrée en vigueur

10. La présente norme ISA est applicable aux audits d'états financiers pour les périodes ouvertes à compter du 15 décembre 2021.

Objectif

11. L'objectif de l'auditeur est d'identifier et d'évaluer les risques d'anomalies significatives, provenant de fraudes ou résultant d'erreurs, au niveau des états financiers et au niveau des assertions, fournissant ainsi une base pour concevoir et mettre en œuvre des réponses aux risques évalués d'anomalies significatives.

⁷ Norme ISA 240, *Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers*.

⁸ Norme ISA 330, *Réponses de l'auditeur à l'évaluation des risques*, paragraphe 5.

⁹ Norme ISA 330, paragraphe 6.

¹⁰ Norme ISA 200, paragraphe A65(a).

Définitions

12. Dans les normes ISA, on entend par :

- (a) « assertions » - Déclarations, explicites ou non, relatives à la comptabilisation, l'évaluation, la présentation et les informations à fournir dans les états financiers, qui sont inhérentes à la direction lorsqu'elle déclare que les états financiers ont été préparés conformément au référentiel comptable applicable. , L'auditeur se réfère aux assertions pour examiner les différents types d'anomalies qui peuvent survenir lorsqu'il identifie et évalue les risques d'anomalies significatives et qu'il y répond; (Voir par. A1)
- (b) « risque lié à l'activité » - Risque résultant des conditions, événements, circonstances, décisions ou absence de décisions importants, qui pourraient compromettre la capacité de l'entité à atteindre ses objectifs et à mettre en œuvre ses stratégies, ou résultant de la fixation d'objectifs et de stratégies inappropriés ;
- (c) « contrôles » - Politiques et procédures qu'établit l'entité pour atteindre les objectifs de contrôle de la direction et des personnes constituant le gouvernement d'entreprise. Dans ce contexte : (Voir par. A2–A5)
 - (i) les politiques décrivent ce qu'il faut faire, ou ne pas faire, dans l'entité pour assurer le contrôle. Certaines sont documentées, formulées explicitement dans des communications, ou implicites au travers d't actions et de décisions,
 - (ii) les procédures sont les actions par lesquelles les politiques sont mises en œuvre ;
- (d) « contrôles généraux informatiques » - Contrôles afférents aux processus informatiques de l'entité qui contribuent à assurer de manière permanente le bon fonctionnement de l'environnement informatique, notamment le maintien du fonctionnement efficace des contrôles du traitement de l'information et l'intégrité de celle-ci (c'est-à-dire l'exhaustivité, l'exactitude et la validité de l'information) présente dans le système d'information de l'entité. Voir également la définition d'« environnement informatique » ;
- (e) « contrôles du traitement de l'information » -Contrôles qui concernent le traitement de l'information dans les applications informatiques ou les processus manuels du système d'information de l'entité et qui visent à répondre directement aux risques liés à l'intégrité des informations (c'est-à-dire l'exhaustivité, l'exactitude et la validité des opérations et des autres informations) ; (Voir par. A6)
- (f) « facteurs de risque inhérent » - Caractéristiques d'événements ou de situations ayant une incidence sur la possibilité qu'une assertion portant sur un flux d'opérations, un solde de compte ou une information fournie comporte une anomalie, provenant de fraudes ou résultant d'erreurs, avant prise en considération des contrôles. Ces facteurs peuvent être qualitatifs ou quantitatifs, et incluent la complexité, la subjectivité, le changement, l'incertitude et la possibilité de biais introduits par la direction ou d'autres facteurs de risque de fraude¹¹, dans la mesure où ils influent sur le risque inhérent ; (Voir par. A7–A8)
- (g) « environnement informatique » - Applications informatiques et infrastructure informatique, de même que les processus informatiques et les membres du personnel qui y participent, grâce auxquels l'entité mène à bien ses activités et ses stratégies. Dans la présente norme ISA :
 - (i) une application informatique consiste en un programme ou un ensemble de programmes servant au déclenchement, au traitement, à l'enregistrement ou à la communication d'opérations ou d'informations. Les applications informatiques comprennent les entrepôts de données et les générateurs de rapports,
 - (ii) l'infrastructure informatique se compose du réseau, des systèmes d'exploitation et des bases de données ainsi que du matériel et des logiciels connexes,
 - (iii) les processus informatiques sont les processus mis en œuvre par l'entité pour la gestion des accès à l'environnement informatique, des modifications apportées aux programmes ou à l'environnement informatique, et des activités liées à l'informatique ;

¹¹ Norme ISA 240, paragraphes A24–A27.

- (h) « assertions pertinentes » - Assertions portant sur un flux d'opérations, un solde de compte ou une information fournie pour lesquelles un risque d'anomalies significatives est identifié. Lorsque l'auditeur détermine si une assertion est pertinente, il le fait avant prise en considération des contrôles y afférents (c'est-à-dire qu'il tient compte du risque inhérent) ; (Voir par. A9)
- (i) « risques provenant de l'utilisation de l'informatique » - Possibilité que la conception ou le fonctionnement des contrôles du traitement de l'information soit inefficace ou les risques que l'intégrité des informations (c'est-à-dire l'exhaustivité, l'exactitude et la validité des opérations et des autres informations) ne soit pas maintenue au sein du système d'information de l'entité, en raison de l'inefficacité de la conception ou du fonctionnement des contrôles se rapportant aux processus informatiques de l'entité (voir la définition d'« environnement informatique ») ;
- (j) « procédures d'évaluation des risques » - Procédures d'audit conçues et mises en œuvre pour identifier et évaluer les risques d'anomalies significatives, que celles-ci proviennent de fraudes ou résultent d'erreurs, au niveau des états financiers et des assertions ;
- (k) « flux d'opérations important, solde de compte important ou information fournie importante » - Flux d'opérations, solde de compte ou information fournie concerné par une ou plusieurs assertions pertinentes ;
- (l) « risque important » - Risque d'anomalies significatives identifié, : (Voir par. A10)
 - (i) pour lequel l'évaluation du risque inhérent pour ce risque d'anomalies significatives se situe près de l'extrémité supérieure de l'échelle de risque inhérent en raison de la mesure dans laquelle les facteurs de risque inhérent influent sur la combinaison que forment la probabilité qu'une anomalie se produise et l'ampleur qu'elle pourrait prendre, le cas échéant, ou
 - (ii) le risque d'anomalies significatives qui doit, selon les diligences d'autres normes ISA, être considéré comme un risque important¹² ;
- (m) « système de contrôle interne » - Système dont la conception, la mise en œuvre et le maintien sont assurés par les personnes constituant le gouvernement d'entreprise, la direction et d'autres membres du personnel et dont l'objet est de fournir une assurance raisonnable quant à la réalisation des objectifs de l'entité en ce qui concerne la fiabilité de son information financière, l'efficacité et l'efficience de ses activités et la conformité aux textes législatifs et réglementaires applicables. Pour les besoins des normes ISA, le système de contrôle interne comporte les cinq composantes interreliées suivantes :
 - (i) environnement de contrôle,
 - (ii) processus d'évaluation des risques par l'entité,
 - (iii) processus de suivi du système de contrôle interne par l'entité,
 - (iv) système d'information et de communication,
 - (v) mesures de contrôle.

Diligences requises

Procédures d'évaluation des risques et procédures liées

13. L'auditeur doit concevoir et mettre en œuvre des procédures d'évaluation des risques lui permettant de recueillir des éléments probants procurant une base appropriée pour : (Voir par. A11–A18)
 - (a) l'identification et l'évaluation des risques d'anomalies significatives, que celles-ci proviennent de fraudes ou résultent d'erreurs, au niveau des états financiers et des assertions ;
 - (b) la conception, conformément à la norme ISA 330, de procédures d'audit complémentaires.

¹² Norme ISA 240, paragraphe 27 et norme ISA 550, *Parties liées*, paragraphe 18.

L'auditeur doit concevoir et mettre en œuvre des procédures d'évaluation des risques en évitant tout biais qui favoriserait l'obtention d'éléments probants corroborants ou l'exclusion d'éléments probants contradictoires. (Voir par. A14)

14. Les procédures d'évaluation des risques doivent notamment comprendre : (Voir par. A19–A21)
- (a) des demandes d'informations auprès de la direction et d'autres personnes appropriées au sein de l'entité, dont les membres de la fonction d'audit interne (lorsque cette fonction existe) ; (Voir par. A22–A26)
 - (b) des procédures analytiques ; (Voir par. A27–A31)
 - (c) l'observation physique et l'inspection. (Voir par. A32–A36)

Informations provenant d'autres sources

15. Pour recueillir des éléments probants conformément au paragraphe 13, l'auditeur doit prendre en considération les informations obtenues dans le cadre : (Voir par. A37–A38)
- (a) des procédures qu'il a mises en œuvre relativement à l'acceptation ou au maintien de la relation client ou de la mission d'audit ;
 - (b) d'autres missions réalisées auprès de l'entité par l'associé responsable de la mission, le cas échéant.
16. Lorsque l'auditeur prévoit l'utilisation d'informations recueillies à partir de son expérience passée auprès de l'entité et des procédures réalisées au cours des audits précédents, il doit évaluer si, en tant qu'éléments probants pour l'audit en cours, ces informations demeurent pertinentes et fiables. (Voir par. A39–A41)

Entretiens entre les membres de l'équipe affectés à la mission

17. L'associé responsable de la mission et les autres membres-clés de l'équipe affectés à la mission doivent s'entretenir de l'application du référentiel comptable applicable ainsi que la possibilité que les états financiers de l'entité comportent des anomalies significatives. (Voir par. A42–A47)
18. Lorsque certains membres de l'équipe affectés à la mission ne participent pas à l'entretien, l'associé responsable de la mission doit déterminer quels sont les sujets qu'il convient de leur communiquer.

Prise de connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité (Voir par. A48–A49)

Prise de connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable (Voir par. A50–A55)

19. L'auditeur doit mettre en œuvre des procédures d'évaluation des risques afin d'acquérir une connaissance :
- (a) des aspects suivants de l'entité et de son environnement :
 - (i) la structure organisationnelle de l'entité, la détention du capital et ses structures de gouvernance ainsi que son modèle économique, incluant la mesure dans laquelle le recours à l'informatique y est intégré, (Voir par. A56–A67)
 - (ii) les facteurs relatifs au secteur d'activité, les facteurs réglementaires et les autres facteurs externes pertinents, (Voir par. A68–A73)
 - (iii) les mesures utilisées par l'entité ou par des parties externes afin d'évaluer la performance financière de l'entité ; (Voir par. A74–A81)

- (b) du référentiel comptable applicable, des méthodes comptables retenues par l'entité et, le cas échéant, des raisons des changements apportés ; (Voir par. A82–A84)
- (c) de la manière, dont les facteurs de risque inhérent influent sur la possibilité que les assertions portant sur des flux d'opérations, des soldes de comptes ou des informations à fournir comportent des anomalies et dans quelle mesure ils influent sur cette possibilité : ceci dans le cadre de la préparation des états financiers conformément au référentiel comptable applicable et au regard de sa connaissance des éléments énoncés aux paragraphes (a) et (b). (Voir par. A85–A89)

20. L'auditeur doit évaluer si les méthodes comptables de l'entité sont appropriées et si elles sont conformes au référentiel comptable applicable.

Prise de connaissance des composantes du système de contrôle interne de l'entité (Voir par. A90–A95)

L'environnement de contrôle, le processus d'évaluation des risques par l'entité et le processus de suivi du système de contrôle interne par l'entité (Voir par. A96–A98)

L'environnement de contrôle

21. L'auditeur doit prendre connaissance de l'environnement de contrôle pertinent pour la préparation des états financiers en mettant en œuvre des procédures d'évaluation des risques visant à : (Voir par. A99–A100)	
<p>(a) comprendre l'ensemble des contrôles, des processus et de l'organisation prenant en compte : (Voir par. A101– A102)</p> <ul style="list-style-type: none"> (i) la façon dont la direction s'acquitte de ses responsabilités de surveillance, notamment en ce qui concerne la culture de l'entité et l'importance que la direction attache à l'intégrité et aux valeurs éthiques, (ii) l'indépendance des personnes constituant le gouvernement d'entreprise et la surveillance qu'ils exercent à l'égard du système de contrôle interne de l'entité, lorsqu'ils ne sont pas membres de la direction, (iii) l'attribution des pouvoirs et des responsabilités par l'entité, (iv) la manière dont l'entité recrute, perfectionne et retient les personnes compétentes, (v) la manière dont l'entité demande aux personnes ayant des responsabilités concernant le système de contrôle interne de lui rendre des comptes sur la réalisation des objectifs de ce système ; 	<p>(b) évaluer : (Voir par. A103–A108)</p> <ul style="list-style-type: none"> (i) si la direction, sous la surveillance des personnes constituant le gouvernement d'entreprise, a développé et entretient une culture d'honnêteté et de comportement éthique, (ii) si l'environnement de contrôle fournit une base appropriée, compte tenu de la nature et de la complexité de l'entité, sur laquelle peuvent s'appuyer les autres composantes du système de contrôle interne de l'entité, (iii) si les déficiences de contrôle relevées dans l'environnement de contrôle affaiblissent les autres composantes du système de contrôle interne de l'entité.

Le processus d'évaluation des risques par l'entité

22. L'auditeur doit prendre connaissance du processus d'évaluation des risques par l'entité pertinent pour la préparation des états financiers en mettant en œuvre des procédures d'évaluation des risques visant à :	
<p>(a) comprendre le processus suivi par l'entité pour : (Voir par. A109–A110)</p>	<p>(b) évaluer si le processus d'évaluation des risques par l'entité est approprié aux circonstances de l'entité, compte tenu de la nature et de la complexité de celle-ci. (Voir par. A111–A113)</p>

<ul style="list-style-type: none"> (i) identifier les risques liés à l'activité qui sont pertinents au regard des objectifs de l'information financière (Voir par. A62) (ii) évaluer l'importance de ces risques, y compris leur probabilité de réalisation, (iii) répondre à ces risques ; 	
--	--

23. Lorsque l'auditeur identifie des risques d'anomalies significatives que la direction n'a pas identifiés, il doit :

- (a) déterminer si ces risques auraient normalement dû être identifiés dans le cadre du processus d'évaluation des risques par l'entité et, si tel est le cas, prendre connaissance des raisons pour lesquelles ces risques n'ont pu être identifiés dans le cadre de ce processus ;
- (b) considérer les conséquences que cela peut avoir sur l'évaluation qu'il est tenu de faire selon le paragraphe 22 (b)

Le processus de suivi du système de contrôle interne par l'entité

<p>24. L'auditeur doit prendre connaissance du processus mis en œuvre par l'entité pour le suivi du système de contrôle interne pertinent pour la préparation des états financiers en mettant en œuvre des procédures d'évaluation des risques visant à: (Voir par. A114–A115)</p>	
<ul style="list-style-type: none"> (a) comprendre les aspects du processus de l'entité traitant : <ul style="list-style-type: none"> (i) les évaluations continues et ponctuelles visant à effectuer le suivi de l'efficacité des contrôles, ainsi qu'à l'identification et à la correction des déficiences de contrôle relevées; et (Voir par. A116–A117) (ii) à la fonction d'audit interne de l'entité (lorsque cette fonction existe), notamment sa nature, ses responsabilités et ses activités ; (Voir par. A118) (b) comprendre les sources des informations utilisées dans le cadre du processus de suivi du système de contrôle interne par l'entité, et les fondements sur lesquels la direction s'appuie pour apprécier si les informations sont suffisamment fiables pour répondre aux objectifs de ce suivi; (Voir par. A119 et A120) 	<p>et</p> <ul style="list-style-type: none"> (c) 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. (Voir par. A121–A122)

Système d'information et de communication, et mesures de contrôle (Voir par. A123–A130)

Le système d'information et de communication

<p>25. L'auditeur doit prendre connaissance du système d'information et de communication de l'entité pertinents pour la préparation des états financiers en mettant en œuvre des procédures d'évaluation des risques visant à: (Voir par. A131)</p>	
<ul style="list-style-type: none"> (a) comprendre les activités de traitement de l'information de l'entité, incluant ses données et ses informations, les ressources devant servir à mener ces activités et les politiques qui définissent, pour les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes : (Voir par. A132– A143) (i) le flux des informations dans le système d'information de l'entité, y compris : 	<p>Et</p> <ul style="list-style-type: none"> (c) évaluer si le système d'information et la communication de l'entité contribuent adéquatement à la préparation des états financiers de l'entité conformément au référentiel comptable applicable. (Voir par. A146)

<p>a. comment les opérations sont initiées et comment les informations les concernant sont enregistrées, traitées, corrigées (au besoin), reportées dans le grand livre et communiquées dans les états financiers ; et</p> <p>b. comment les informations sur des événements et des circonstances, autres que les opérations, sont saisies, traitées et fournies dans les états financiers,</p> <p>(ii) les enregistrements comptables, les postes spécifiques des états financiers et les autres pièces justificatives qui concernent le flux des informations dans le système d'information,</p> <p>(iii) le processus d'élaboration de l'information financière utilisé pour préparer les états financiers de l'entité, y compris les informations à fournir,</p> <p>(iv) les ressources de l'entité, y compris son environnement informatique, qui sont pertinentes au regard des paragraphes (a)(i)–(a)(iii) ci-dessus ;</p> <p>(b) comprendre comment s'effectue la communication des éléments importants pour la préparation des états financiers et des responsabilités connexes relatives au système d'information et aux autres composantes du système de contrôle interne entre : (Voir par. A144– A145)</p> <p>(i) les personnes au sein de l'entité, y compris la communication des rôles et des responsabilités en matière d'information financière,</p> <p>(ii) la direction et les personnes constituant le gouvernement d'entreprise,</p> <p>(iii) l'entité et les parties externes, par exemple les autorités de contrôle ;</p>	
---	--

Mesures de contrôle

<p>26. L'auditeur doit prendre connaissance de la composante « mesures de contrôle » en mettant en œuvre des procédures d'évaluation des risques visant à : (Voir par. A147–A157)</p>	
<p>(a) identifier les contrôles de la composante « mesures de contrôle » afin de répondre aux risques d'anomalies significatives au niveau des assertions, c'est-à-dire :</p> <p>(i) les contrôles qui répondent à un risque qualifié comme étant un risque important, (Voir par. A158–A159)</p> <p>(ii) les contrôles relatifs aux écritures comptables, y compris les écritures non standard utilisées pour comptabiliser des opérations non récurrentes ou inhabituelles, ou des ajustements, (Voir par. A160– A161)</p> <p>(iii) les contrôles pour lesquels l'auditeur prévoit de tester l'efficacité du fonctionnement en vue de déterminer la nature, le calendrier et l'étendue des tests de substance, ce qui doit inclure les contrôles</p>	<p>Et</p> <p>(d) pour chaque contrôle identifié au paragraphe (a) ou (c)(ii) : (Voir par. A175–A181)</p> <p>(i) évaluer si la conception du contrôle est efficace pour permettre de répondre aux risques d'anomalies significatives au niveau des assertions, ou pour permettre le fonctionnement d'autres contrôles ; et</p> <p>(ii) déterminer si le contrôle a été mis en œuvre,</p>

<p>visant à répondre aux risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés ; et (Voir par. A162– A164)</p> <p>(iv) les autres contrôles qui, selon le jugement professionnel de l'auditeur, sont appropriés pour permettre à celui-ci d'atteindre les objectifs énoncés au paragraphe 13 relatifs aux risques au niveau des assertions ; (Voir par. A165)</p> <p>(b) identifier, sur la base des contrôles identifiés au paragraphe a), les applications informatiques et les autres aspects de l'environnement informatique qui sont sujets aux risques provenant du recours à l'informatique ; (Voir par. A166–A172)</p> <p>(c) identifier, en ce qui concerne les applications informatiques et les autres aspects de l'environnement informatique identifiés au paragraphe b) : (Voir par. A173–A174)</p> <p>(i) les risques s'y rapportant, provenant du recours à l'informatique; et</p> <p>(ii) les contrôles généraux sur le système informatique visant à répondre à ces risques ;</p>	<p>en exécutant d'autres procédures complémentaires à ses demandes d'informations auprès du personnel de l'entité.</p>
--	--

Déficiences de contrôle dans le système de contrôle interne de l'entité

27. Sur la base de son évaluation de chacune des composantes du système de contrôle interne de l'entité, l'auditeur doit déterminer si une ou plusieurs déficiences de contrôle a ou ont été identifiées(s). (Voir par. A182–A183)

Identification et évaluation des risques d'anomalies significatives (Voir par. A184–A185)

Identification des risques d'anomalies significatives

28. L'auditeur doit identifier les risques d'anomalies significatives et déterminer s'ils existent : (Voir par. A186–A192)
- (a) au niveau des états financiers ; (Voir par. A193–A200)
 - (b) au niveau des assertions retenues pour les flux d'opérations, les soldes de comptes ou les informations à fournir. (Voir par. A201)
29. L'auditeur doit déterminer les assertions pertinentes ainsi que les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes qui y sont associés. (Voir par. A202–A204)

Évaluation des risques d'anomalies significatives au niveau des états financiers

30. Concernant les risques d'anomalies significatives qu'il a identifiés au niveau des états financiers, l'auditeur doit les évaluer et : (Voir par. A193–A200)
- (a) déterminer s'ils ont une incidence sur son évaluation des risques au niveau des assertions ; et
 - (b) évaluer la nature et l'étendue de leur effet diffus sur les états financiers.

Évaluation des risques d'anomalies significatives au niveau des assertions

Évaluation du risque inhérent (Voir par. A205–A217)

31. Concernant les risques d'anomalies significatives qu'il a identifiés au niveau des assertions, l'auditeur doit évaluer le risque inhérent en déterminant la probabilité et l'ampleur des anomalies. Pour y procéder, l'auditeur doit tenir compte de la façon, et la mesure dans laquelle :
- (a) les facteurs de risque inhérent ont une incidence sur la possibilité que les assertions pertinentes comportent des anomalies ; et
 - (b) les risques d'anomalies significatives au niveau des états financiers ont une incidence sur l'évaluation du risque inhérent sur les risques d'anomalies significatives au niveau des assertions. (Voir par. A215–A216)
32. L'auditeur doit déterminer s'il existe des risques importants parmi les risques d'anomalies significatives évalués. (Voir par. A218–A221)
33. L'auditeur doit déterminer s'il y existe des risques d'anomalies significatives au niveau des assertions pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés. (Voir par. A222–A225)

Évaluation du risque lié au contrôle interne

34. Si l'auditeur prévoit de tester l'efficacité du fonctionnement des contrôles, il doit évaluer le risque lié au contrôle interne. S'il ne prévoit pas de tester l'efficacité du fonctionnement des contrôles, l'évaluation de l'auditeur du risque lié au contrôle interne doit faire en sorte que l'évaluation du risque d'anomalies significatives soit identique à celle de l'évaluation du risque inhérent. (Voir par. A226– A229)

Évaluation des éléments probants recueillis au moyen des procédures d'évaluation des risques

35. L'auditeur doit évaluer si les éléments probants recueillis au moyen des procédures d'évaluation des risques procurent une base appropriée pour l'identification et l'évaluation des risques d'anomalies significatives. Dans la négative, il doit mettre en œuvre des procédures supplémentaires d'évaluation des risques jusqu'à ce qu'il obtienne des éléments probants qui fournissent une telle base. Lorsqu'il identifie et évalue les risques d'anomalies significatives, l'auditeur doit tenir compte de tous les éléments probants recueillis au moyen des procédures d'évaluation des risques, que ces éléments corroborent ou contredisent les assertions de la direction. (Voir par. A230–A232)

Flux d'opérations, soldes de comptes et informations à fournir qui, sans être importants, sont significatifs

36. Concernant les flux d'opérations, les soldes de comptes et les informations à fournir qui sont significatifs, mais qu'il a évalués comme non importants, l'auditeur doit établir si son évaluation demeure appropriée. (Voir par. A233–A235)

Révision de l'évaluation des risques

37. Si l'auditeur obtient de nouvelles informations qui sont incohérentes avec les éléments probants sur lesquels il s'est fondé pour procéder à l'identification ou à l'évaluation initiales des risques d'anomalies significatives, il doit réviser cette identification ou cette évaluation. (Voir par. A236)

Documentation

38. L'auditeur doit consigner dans la documentation de l'audit¹³ : (Voir par. A237–A241)

¹³ Norme ISA 230, *Documentation de l'audit*, paragraphes 8–11, A6–A7.

- (a) les entretiens entre les membres de l'équipe affectés à la mission ainsi que les décisions importantes prises à l'issue de ces entretiens ;
- (b) les éléments clés de la connaissance qu'il a acquise conformément aux paragraphes 19, 21, 22, 24 et 25, les sources d'informations qui lui ont permis d'acquérir cette connaissance, et les procédures d'évaluation des risques mises en œuvre ;
- (c) l'évaluation de la conception des contrôles identifiés et la vérification de leur mise en œuvre, conformément aux diligences du paragraphe 26 ; et
- (d) les risques d'anomalies significatives qu'il a identifiés et évalués au niveau des états financiers et au niveau des assertions, y compris les risques importants et les risques pour lesquels les contrôles de substance ne peuvent fournir, à eux seuls, des éléments probants suffisants et appropriés, ainsi que la logique qui sous-tend les jugements importants portés.

Modalités d'application et autres commentaires explicatifs

Définitions (Voir par. 12)

Assertions (Voir par. 12(a))

- A1. Lorsqu'il identifie et évalue les risques d'anomalies significatives et qu'il y répond, l'auditeur se réfère aux catégories d'assertions pour examiner les différents types d'anomalies susceptibles de se produire. Des exemples de catégories d'assertions sont fournis au paragraphe A190. Les assertions sont différentes des déclarations écrites que la direction fournit à l'auditeur, comme le requiert la norme ISA 580¹⁴, pour confirmer certains points ou étayer d'autres éléments probants.

Contrôles (Voir par. 12(c))

- A2. Les contrôles font partie intégrante des composantes du système de contrôle interne de l'entité.
- A3. Les politiques sont mises en œuvre au travers d'actions que pose le personnel de l'entité, ou par des actions que celui-ci évite de poser parce qu'elles vont à l'encontre de ces politiques.
- A4. Les procédures peuvent être imposées par des documents officiels ou par d'autres communications émanant de la direction ou des personnes constituant le gouvernement d'entreprise, ou être le résultat de comportements qui, sans être imposés, sont conditionnés par la culture de l'entité. Des procédures peuvent être exécutées au travers d'actions autorisées par des applications informatiques de l'entité, ou reposer sur d'autres aspects de l'environnement informatique de l'entité.
- A5. Les contrôles peuvent être directs ou indirects. Les contrôles directs sont des contrôles qui sont suffisamment précis pour permettre de répondre aux risques d'anomalies significatives au niveau des assertions, tandis que les contrôles indirects visent à favoriser le fonctionnement des contrôles directs.

Contrôles du traitement de l'information (Voir par. 12(e))

- A6. Les risques liés à l'intégrité des informations découlent de la possibilité que les politiques en matière d'information de l'entité (c'est-à-dire les politiques qui définissent les flux d'information, les documents et les processus d'information du système d'information de l'entité) ne soient pas mises en œuvre efficacement. Les contrôles du traitement de l'information sont des procédures qui favorisent la mise en œuvre efficace de ces politiques. Ils peuvent être automatisés (c'est-à-dire intégrés aux applications informatiques) ou manuels (par exemple, les contrôles sur les données d'entrée ou de sortie), et dépendre d'autres contrôles (par exemple, de contrôles généraux informatiques ou d'autres contrôles du traitement de l'information).

¹⁴ Norme ISA 580, *Déclarations écrites*.

Facteurs de risque inhérent (Voir par. 12(f))

L'Annexe 2 fournit d'autres exemples d'éléments à prendre en considération pour comprendre les facteurs de risque inhérents.

- A7. Les facteurs de risque inhérent sont des facteurs qualitatifs ou quantitatifs ayant une incidence sur la possibilité que des assertions comportent des anomalies. Des exemples de facteurs de risque inhérent qualitatifs qui concernent la préparation de l'information exigée par le référentiel comptable applicable comprennent :
- la complexité ;
 - la subjectivité ;
 - le changement ;
 - l'incertitude ou ;
 - la possibilité d'anomalies résultant de biais introduit par la direction ou d'autres facteurs de risque de fraude, dans la mesure où ils influencent le risque inhérent.
- A8. D'autres exemples de facteurs de risque inhérent ayant une incidence sur la possibilité qu'une assertion concernant un flux d'opérations, un solde de compte ou une information à fournir comporte une anomalie, sont :
- l'importance quantitative ou qualitative du flux d'opérations, du solde de compte ou de l'information à fournir ;
 - le volume ou le manque d'homogénéité des éléments à traiter dans la catégorie d'opérations ou dans le solde de compte, ou à refléter dans l'information à fournir.

Assertions pertinentes (Voir par. 12(h))

- A9. Un risque d'anomalies significatives peut affecter plus d'une assertion, auquel cas toutes les assertions à l'égard desquelles il existe un tel risque sont des assertions pertinentes. Une assertion pour laquelle aucun risque d'anomalies significatives n'est identifié ne constitue pas une assertion pertinente.

Risque important (Voir par. 12(l))

- A10. L'importance, qui peut être décrite comme le poids relatif d'un élément, est établie par l'auditeur dans le contexte dans lequel l'élément est considéré. Lorsqu'il évalue l'importance aux fins de l'évaluation du risque inhérent, l'auditeur peut se demander comment et dans quelle mesure les facteurs de risque inhérent influent sur la combinaison que forment la probabilité qu'une anomalie se produise et l'ampleur de l'anomalie potentielle si celle-ci se produit.

Procédures d'évaluation des risques et procédures liées (Voir par. 13–18)

- A11. Les risques d'anomalies significatives à identifier et à évaluer comprennent aussi bien ceux résultant d'erreurs que ceux provenant de fraudes, et sont couverts par la présente Norme ISA. Cependant, l'importance de la fraude est telle que les diligences requises et les modalités d'application complémentaires sont prévues dans la Norme ISA 240 en relation avec les procédures d'évaluation des risques et des mesures de contrôle, afin de recueillir des informations qui sont utilisées pour identifier les risques d'anomalies significatives provenant de fraudes¹⁵. En outre, les normes ISA suivantes fournissent d'autres diligences et modalités d'application se rapportant à l'identification et à l'évaluation des risques d'anomalies significatives concernant des points précis ou de circonstances particulières:

¹⁵ Norme ISA 240, paragraphes 12–27.

- la norme ISA 540 (révisée)¹⁶, pour les estimations comptables ;
- la norme ISA 550, pour les relations et les opérations avec les parties liées ;
- la norme ISA 570 (révisée)¹⁷, pour la continuité de l'exploitation ;
- la norme ISA 600¹⁸, pour les états financiers d'un groupe.

A12. L'esprit critique est nécessaire pour l'évaluation appropriée des éléments probants recueillis lors de la mise en œuvre des procédures d'évaluation des risques, et aide l'auditeur à rester tout aussi attentif aux éléments probants qui corroborent qu'à ceux qui contredisent l'existence de risques, en évitant tout biais. L'esprit critique est une attitude qu'adopte l'auditeur lorsqu'il porte des jugements professionnels qui lui procure alors une base pour ses travaux. L'auditeur exerce son jugement professionnel pour déterminer à quel moment il dispose d'éléments probants qui lui procure une base appropriée pour l'évaluation des risques.

A13. L'auditeur fait notamment preuve d'esprit critique lorsqu'il :

- remet en question les informations contradictoires ainsi que la fiabilité des documents ;
- examine les réponses aux demandes d'informations et les autres renseignements obtenus de la direction et des personnes constituant le gouvernement d'entreprise ;
- est attentif aux conditions qui peuvent indiquer de possibles anomalies, que celles-ci résultent de fraudes ou proviennent d'erreurs ;
- détermine si les éléments probants recueillis étayent son identification et son évaluation des risques d'anomalies significatives, compte tenu de la nature et des circonstances de l'entité.

Importance d'éviter tout biais lors de l'obtention d'éléments probants (Voir par. 13)

A14. Le fait de concevoir et de mettre en œuvre des procédures d'évaluation des risques permettant d'obtenir, en évitant tout biais, des éléments probants étayant l'identification et l'évaluation des risques d'anomalies significatives aide l'auditeur à déceler les informations potentiellement contradictoires, ce qui peut aider l'auditeur à faire preuve d'esprit critique lors de l'identification et l'évaluation des risques d'anomalies significatives.

Sources d'éléments probants (Voir par. 13)

A15. Concevoir et mettre en œuvre des procédures d'évaluation des risques permettant de recueillir des éléments probants en évitant tout biais, peut nécessiter de l'auditeur de recueillir des éléments à partir de multiples sources internes et externes à l'entité. Cependant, il n'est pas tenu de mener des recherches exhaustives pour identifier toutes les sources possibles d'éléments probants. Outre les informations provenant d'autres sources¹⁹, l'auditeur peut utiliser, dans le cadre de ses procédures d'évaluation des risques :

- des informations provenant de ses interactions avec la direction, les personnes constituant le gouvernement d'entreprise et d'autres membres clés du personnel de l'entité (par exemple, les auditeurs internes) ;
- des informations obtenues directement ou indirectement de parties externes (par exemple, des autorités de contrôle) ;
- des informations sur l'entité qui sont accessibles au public, comme les communiqués de presse de l'entité, les documents qui sont destinés aux analystes ou qui concernent les présentations à l'intention des groupes d'investisseurs, les rapports produits par des analystes ou les informations boursières.

¹⁶ Norme ISA 540 (révisée), *Audit des estimations comptables et des informations les concernant*.

¹⁷ Norme ISA 570 (révisée), *Continuité de l'exploitation*.

¹⁸ Norme ISA 600, *Audits d'états financiers de groupe (y compris l'utilisation des travaux des auditeurs des composantes) — Considérations particulières*.

¹⁹ Voir les paragraphes A37–A38.

Peu importe la source d'information, l'auditeur tient compte de la pertinence et de la fiabilité des informations devant servir comme éléments probants, conformément à la norme ISA 500²⁰.

Application proportionnée (Voir par. 13)

- A16. La nature et l'étendue des procédures d'évaluation des risques variera en fonction de la nature et des circonstances de l'entité (par exemple, la formalisation ou non de politiques et procédures, des processus et des systèmes). L'auditeur exerce son jugement professionnel pour déterminer la nature et l'étendue des procédures d'évaluation des risques à mettre en œuvre pour satisfaire aux diligences de la présente norme ISA.
- A17. Bien que le niveau de formalisation des politiques et procédures, des processus et des systèmes de l'entité puisse varier, l'auditeur est tenu de prendre connaissance conformément aux paragraphes 19–22 et 24–26.

Exemples :

Certaines entités, notamment des entités peu complexes (et en particulier les entités gérées par un propriétaire-dirigeant), peuvent ne pas avoir établi de processus et de systèmes structurés (tel qu'un processus d'évaluation des risques ou de suivi du système de contrôle interne), ou qu'elles aient établi des processus ou des systèmes documentés de manière succincte ou qui ne sont pas mis en œuvre de façon uniforme. En l'absence de systèmes et de processus formalisés, l'auditeur peut tout de même être en mesure de mettre en œuvre des procédures d'évaluation des risques en procédant à des observations physiques et à des demandes d'informations.

On s'attend à ce que les autres entités, notamment les entités plus complexes, aient établi et plus formalisé des politiques et procédures structurées. L'auditeur peut examiner cette documentation lors de la mise en œuvre des procédures d'évaluation des risques.

- A18. La nature et l'étendue des procédures d'évaluation des risques à mettre en œuvre lors d'une première mission peuvent être plus développées que lors d'une mission récurrente. Par la suite, l'auditeur pourra axer ses procédures sur les changements survenus depuis la période précédente.

Types de procédures d'évaluation des risques (Voir par. 14)

- A19. Les différents types de procédures d'audit qu'il est possible de mettre en œuvre afin d'obtenir des éléments probants, qu'il s'agisse de procédures d'évaluation des risques ou de procédures d'audit complémentaires, sont décrits dans la norme ISA 500²¹. Le fait que certaines données comptables et d'autres éléments probants soient disponibles uniquement sous forme électronique, ou seulement à certains moments, peut avoir une incidence sur la nature, le calendrier et l'étendue des procédures d'audit²². S'il s'avère que c'est efficace, l'auditeur peut exécuter, en même temps que des procédures d'évaluation des risques, des contrôles de substance ou des tests de procédures conformément à la norme ISA 330. Les éléments probants recueillis pourront servir non seulement à l'identification et à l'évaluation des risques d'anomalies significatives, mais aussi à la détection des anomalies au niveau des assertions ou à l'évaluation de l'efficacité du fonctionnement des contrôles.
- A20. Bien que l'auditeur soit tenu de mettre en œuvre l'ensemble des procédures d'évaluation des risques décrites au paragraphe 14 dans le cadre de la prise de connaissance requise de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité (voir les paragraphes 19–26), il n'est pas tenu de mettre toutes ces procédures en œuvre pour chacun des aspects de cette connaissance. D'autres procédures peuvent être mises en œuvre si les informations à obtenir peuvent aider à identifier les risques d'anomalies significatives. Ces procédures peuvent comprendre, par exemple, des demandes d'informations auprès du conseiller

²⁰ Norme ISA 500, *Éléments probants*, paragraphe 7.

²¹ Norme ISA 500, paragraphes A14–A17 et A21–A25.

²² Norme ISA 500, paragraphe A12.

juridique externe de l'entité ou des autorités externes, ou auprès des experts en évaluation auxquels l'entité a fait appel.

Outils et techniques automatisés (Voir par. 14)

A21. L'auditeur peut recourir à des outils ou à des techniques automatisés pour mettre en œuvre des procédures d'évaluation des risques relatives à de grandes quantités de données (telles que les données provenant du grand livre et des journaux auxiliaires ainsi que les autres données opérationnelles), incluant des analyses, des contrôles arithmétiques, des réexecutions et des rapprochements.

Demandes d'informations auprès de la direction et d'autres personnes au sein de l'entité (Voir par. 14(a))

Raisons pour lesquelles l'auditeur procède à des demandes d'informations auprès de la direction et d'autres personnes au sein de l'entité

A22. Les demandes d'informations auprès de la direction et des responsables de l'information financière peuvent permettre à l'auditeur d'obtenir des informations qui lui fourniront une base appropriée pour l'identification et l'évaluation des risques et pour la conception de procédures d'audit complémentaires.

A23. Les demandes d'informations auprès de la direction, des responsables de l'information financière et d'autres personnes appropriées au sein de l'entité, dont des employés de différents niveaux hiérarchiques, peuvent aussi permettre à l'auditeur d'obtenir divers points de vue qui lui seront utiles pour identifier et évaluer les risques d'anomalies significatives.

Exemples :

- Des demandes d'informations auprès des personnes constituant le gouvernement d'entreprise peuvent aider l'auditeur à comprendre l'étendue de la surveillance que ceux-ci exercent à l'égard de la préparation des états financiers par la direction. La Norme ISA 260 (Révisée)²³ souligne l'importance d'un échange réciproque efficace pour aider l'auditeur à obtenir des informations à cet égard auprès des personnes constituant le gouvernement d'entreprise .
- Des demandes d'informations auprès des membres du personnel responsables d'initier, de traiter ou d'enregistrer des opérations complexes ou inhabituelles peuvent aider l'auditeur dans l'appréciation du caractère approprié du choix et de l'application de certaines méthodes comptables suivies .
- Des demandes d'informations auprès du conseil juridique interne de l'entité peuvent fournir des renseignements sur des sujets tels que les litiges, la conformité aux textes législatifs et réglementaires, la connaissance de fraudes commises ou suspectées affectant l'entité, les garanties accordées, les engagements après-ventes, les accords (tels que l'existence de co-entreprises) ou encore la portée des clauses d'un contrat .
- Des demandes d'informations auprès du personnel du service marketing ou commercial peuvent fournir des renseignements sur les évolutions dans la stratégie marketing de l'entité, l'évolution des ventes ou les accords commerciaux avec les clients .
- Des demandes d'informations auprès de la fonction de gestion des risques (ou des personnes qui endossent ce rôle) peuvent fournir des renseignements sur les risques opérationnels et les risques découlant de la réglementation qui peuvent avoir une incidence sur l'élaboration de l'information financière.
- Des demandes d'informations auprès du personnel en charge des systèmes d'information peuvent fournir des renseignements sur les modifications apportées aux systèmes, les défaillances des systèmes ou des contrôles, ou sur d'autres risques liés aux systèmes d'informations.

²³ Norme ISA 260 (Révisée), *Communication avec les personnes constituant le gouvernement d'entreprise*, paragraphe 4(b).

Considérations propres aux entités du secteur public

A24. Lorsqu'il procède à des demandes d'informations auprès de personnes susceptibles de détenir de l'information qui pourrait l'aider à identifier les risques d'anomalies significatives, l'auditeur d'une entité du secteur public peut se tourner vers d'autres sources et adresser ses demandes d'informations aux auditeurs qui, par exemple, ont participé à des audits de performance et à d'autres audits concernant l'entité.

Demandes d'informations auprès de la fonction d'audit interne

L'**Annexe 4** fournit des exemples d'éléments à prendre en considération pour comprendre la fonction d'audit interne de l'entité.

Raisons pour lesquelles l'auditeur procède à des demandes d'informations auprès de la fonction d'audit interne (lorsque cette fonction existe)

A25. Si l'entité a une fonction d'audit interne, les demandes d'informations auprès des personnes appropriées au sein de cette fonction peuvent aider l'auditeur à comprendre l'entité et son environnement ainsi que son système de contrôle interne, aux fins de l'identification et de l'évaluation des risques.

Considérations propres aux entités du secteur public

A26. Les auditeurs des entités du secteur public ont souvent des responsabilités supplémentaires ayant trait au contrôle interne et à la conformité aux textes législatifs et réglementaires applicables. Des demandes d'informations auprès des personnes appropriées qui travaillent au sein de la fonction d'audit interne peuvent aider l'auditeur à identifier les risques de non-conformité significative aux textes législatifs et réglementaires applicables et le risque de déficiences de contrôle relatif à l'élaboration de l'information financière.

Procédures analytiques (Voir par. 14 (b))

Raisons pour lesquelles des procédures analytiques sont mises en œuvre en tant que procédures d'évaluation des risques

A27. Des procédures analytiques sont utiles pour identifier des incohérences, des opérations ou événements inhabituels et des montants, ratios ou tendances pouvant faire apparaître des éléments ayant une incidence sur l'audit. Des corrélations inhabituelles ou inattendues qui sont identifiées peuvent aider l'auditeur à identifier des risques d'anomalies significatives, en particulier des risques d'anomalies significatives provenant de fraudes .

A28. Ainsi, les procédures analytiques mises en œuvre en tant que procédures d'évaluation des risques peuvent aider l'auditeur à identifier et à évaluer les risques d'anomalies significatives en identifiant des aspects de l'entité dont il n'avait pas connaissance ou en lui permettant de comprendre l'incidence des facteurs de risque inhérent, comme le changement, sur la possibilité que les assertions comportent des anomalies.

Types de procédures analytiques

A29. Des procédures analytiques mises en œuvre en tant que procédures d'évaluation des risques peuvent :

- porter à la fois sur des informations tant financières que non financières, par exemple, des corrélations entre les ventes et la surface des espaces de ventes ou le volume des marchandises vendues (informations non financières).

- reposer sur des données agrégées à un niveau global, les résultats de ces procédures analytiques fournissant alors une indication initiale générale sur la probabilité de la présence d'une anomalie significative.

Exemple :

Dans de nombreuses entités, notamment celles dont le modèle économique, les processus ainsi que le système d'information sont peu complexes, l'auditeur peut effectuer une simple comparaison des informations pour avoir une indication des domaines présentant un à risque potentiel plus élevé, L'auditeur peut notamment comparer la variation des soldes de comptes intermédiaires ou mensuels par rapport à celles de périodes antérieures.

- A30. La présente norme ISA traite de l'utilisation par l'auditeur de procédures analytiques en tant que procédures d'évaluation des risques. La norme ISA 520²⁴ traite quant à elle de la mise en œuvre par l'auditeur de procédures analytiques en tant que contrôles de substance (« procédures analytiques de substance ») et de la responsabilité qui incombe à l'auditeur de mettre en œuvre, vers la fin de son audit, des procédures analytiques. Par conséquent, lorsqu'il met en œuvre des procédures analytiques en tant que procédures d'évaluation des risques, l'auditeur n'est pas tenu de se conformer aux diligences de la norme ISA 520. Cependant, les diligences et les modalités d'application de la norme ISA 520 peuvent lui fournir des indications utiles pour la mise en œuvre de procédures analytiques en tant que procédures d'évaluation des risques.

Outils et techniques automatisés

- A31. La mise en œuvre des procédures analytiques peut se faire au moyen d'outils ou de techniques automatisés. L'application de procédures analytiques automatisées à des données est parfois appelée « analyse de données ».

Exemple :

L'auditeur peut se servir d'une feuille de calcul pour comparer les montants budgétés aux montants qui ont réellement été comptabilisés. Il peut aussi mettre en œuvre des procédures plus complexes pour identifier les flux d'opérations, les soldes de comptes ou les informations à fournir à l'égard desquels il pourrait être avisé de mettre en œuvre des procédures d'évaluation des risques particulières, l'auditeur peut procéder à des analyses plus poussées en appliquant des techniques de visualisation à des données extraites du système d'information de l'entité.

Observations physiques et inspections (Voir par. 14 (c))

Raisons pour lesquelles des observations physiques et des inspections sont réalisées en tant que procédures d'évaluation des risques

- A32. Les observations physiques et les inspections peuvent étayer, corroborer ou contredire les informations recueillies auprès de la direction ou d'autres personnes, et peuvent aussi fournir des informations sur l'entité et son environnement.

Application proportionnée

- A33. Lorsque l'entité n'a pas documenté ses politiques et procédures ou que ses contrôles sont peu formalisés, l'auditeur peut encore être en mesure de recueillir des éléments probants à l'appui de l'identification et de l'évaluation des risques d'anomalies significatives au travers d'observations physiques ou d'inspections de l'exécution des contrôles.

²⁴ Norme ISA 520, *Procédures analytiques*.

Exemples :

- L'auditeur peut acquérir, par l'observation directe, une connaissance des contrôles afférents à la prise d'inventaire physique, même si l'entité ne les a pas documentés.
- L'auditeur peut être en mesure d'observer la séparation des tâches.
- L'auditeur peut être en mesure d'observer la saisie des mots de passe.

Observations physiques et inspections réalisées en tant que procédures d'évaluation des risques

A34. Les procédures d'évaluation des risques peuvent inclure des observations physiques et des inspections portant sur :

- les activités de l'entité ;
- des documents internes (tels que les plans d'affaires et les stratégies), les documents comptables et les manuels de contrôle interne ;
- les rapports produits par la direction (par exemple, les rapports de gestion trimestriels et les états financiers intermédiaires) et par les personnes constituant le gouvernement d'entreprise (par exemple, les procès-verbaux des réunions du conseil d'administration) ;
- les établissements et les installations de production de l'entité ;
- les informations provenant de sources externes, notamment les revues de commerce ou d'économie, les rapports rédigés par des analystes, des banques ou des agences de notation, les publications réglementaires ou financières, ou d'autres documents externes qui traitent de la performance financière de l'entité (comme ceux qui sont mentionnés au paragraphe A79) ;
- le comportement et les actions de la direction et des personnes constituant le gouvernement d'entreprise (l'auditeur peut, par exemple, observer une réunion du comité d'audit).

Outils et techniques automatisés

A35. L'auditeur peut aussi recourir à des outils ou à des techniques automatisés, comme des outils d'observation à distance (par exemple, un drone), pour réaliser des observations physiques ou des inspections, surtout en ce qui concerne les actifs.

Considérations propres aux entités du secteur public

A36. Les procédures d'évaluation des risques mises en œuvre par l'auditeur d'une entité du secteur public peuvent aussi comprendre l'observation et l'inspection de documents préparés par la direction à l'intention du pouvoir législatif, comme ceux se rapportant à des obligations d'information sur la performance de l'entité.

Informations provenant d'autres sources (Voir par. 15)

Raisons pour lesquelles l'auditeur prend en considération des informations provenant d'autres sources

A37. Certaines informations provenant d'autres sources peuvent aider l'auditeur à identifier et à évaluer les risques d'anomalies significatives en le renseignant sur :

- la nature de l'entité, les risques liés à l'activité auxquels elle est exposée ainsi que les changements survenus depuis les périodes précédentes ;
- l'intégrité et les valeurs éthiques de la direction et des personnes constituant le gouvernement d'entreprise, ce qui peut aussi lui être utile pour sa connaissance de l'environnement de contrôle ;
- le référentiel comptable applicable et son application au regard de la nature et des circonstances de l'entité.

Autres sources pertinentes

A38. D'autres sources d'information pertinentes comportent :

- les procédures mises en œuvre par l'auditeur relatives à l'acceptation ou au maintien de la relation client ou de la mission d'audit, en application de la norme ISA 220 (révisée)²⁵, ainsi que les conclusions auxquelles elles ont abouti ;
- les autres missions réalisées auprès de l'entité par l'associé responsable de la mission, au cours desquelles celui-ci peut avoir acquis des connaissances pertinentes pour l'audit, notamment en ce qui a trait à l'entité et à son environnement. Il peut s'agir de missions de procédures convenues ou d'autres missions d'audit ou d'assurance, y compris de missions portant sur les informations supplémentaires exigées dans un pays donné.

Informations recueillies par l'auditeur à partir de son expérience passée auprès de l'entité ou acquise au cours d'audits antérieurs (Voir par. 16)

Raisons pour lesquelles les informations recueillies au cours d'audits antérieurs sont importantes pour l'audit en cours

A39. Les informations que l'auditeur a recueillies à partir de son expérience passée auprès de l'entité et à la suite de la mise en œuvre de procédures d'audit au cours d'audits antérieurs peuvent l'aider à déterminer la nature et l'étendue des procédures d'évaluation des risques ainsi qu'à identifier et à évaluer les risques d'anomalies significatives.

Nature des informations recueillies au cours d'audits antérieurs

A40. L'expérience passée auprès de l'entité acquise par l'auditeur et les procédures d'audit réalisées lors des audits précédents peuvent lui fournir des informations sur des sujets tels que :

- L'existence d'anomalies antérieures et le fait qu'elles aient été corrigées ou non en temps voulu.
- La nature de l'entité et de son environnement ainsi que de son contrôle interne (y compris les déficiences de contrôle).
- Les changements importants dans l'entité ou dans ses opérations survenus depuis la clôture de la période précédente.
- Certains types d'opérations et d'autres événements ou de soldes de comptes (et les informations à fournir les concernant) pour lesquels la mise en œuvre des procédures d'audit nécessaires a posé des difficultés, par exemple en raison de leur complexité.

A41. L'auditeur est tenu de déterminer si les informations recueillies à partir de son expérience passée auprès de l'entité et à la suite de la mise en œuvre de procédures d'audit au cours d'audits antérieurs sont toujours pertinentes et fiables lorsqu'il a l'intention de les utiliser dans le cadre de l'audit en cours. Si la nature ou les circonstances de l'entité ont changé ou que de nouvelles informations ont été obtenues, il est possible que les informations obtenues au cours de périodes antérieures ne soient plus pertinentes et fiables pour l'audit en cours. Pour déterminer si des changements sont susceptibles d'affecter la pertinence ou la fiabilité de ces informations, l'auditeur peut procéder à des demandes d'informations et mettre en œuvre d'autres procédures d'audit appropriées, par exemple soumettre les systèmes pertinents à des tests de conformité. Si les informations ne sont plus fiables, il peut envisager de mettre en œuvre des procédures supplémentaires appropriées aux circonstances.

²⁵ Norme ISA 220 (révisée), *Contrôle qualité d'un audit d'états financiers*, paragraphe 12.

Entretiens entre les membres de l'équipe affectés à la mission (Voir par. 17–18)

Raisons pour lesquelles les membres de l'équipe affectés à la mission doivent s'entretenir de l'application du référentiel comptable applicable ainsi que de la possibilité que les états financiers de l'entité comportent des anomalies significatives

A42. Les discussions entre les membres de l'équipe affectés à la mission concernant l'application du référentiel comptable applicable ainsi que de la possibilité que les états financiers de l'entité comportent des anomalies significatives :

- Donnent l'occasion aux membres de l'équipe les plus expérimentés, y compris l'associé responsable de la mission, de partager leur expérience personnelle fondée sur leur connaissance de l'entité, ce qui contribue à une meilleure connaissance de tous les membres de l'équipe affectés à la mission.
- Permettent aux membres de l'équipe affectée à la mission d'échanger des informations sur les risques liés à l'activité auxquels l'entité est exposée, sur la manière dont les facteurs de risque inhérent influent sur la possibilité que des flux d'opérations, des soldes de comptes et des informations à fournir comportent des anomalies, et comment et dans quels domaines les états financiers sont susceptibles de comporter des anomalies significatives provenant de fraudes ou résultant d'erreurs ;
- Aident les membres de l'équipe affectée à la mission à acquérir une meilleure connaissance des potentialités d'anomalies significatives dans les états financiers dans les domaines spécifiques qui leur sont assignés, et à comprendre comment les résultats des procédures d'audit qu'ils ont réalisées peuvent affecter d'autres aspects des travaux d'audit, y compris les décisions relatives à la nature, au calendrier et à l'étendue des procédures d'audit complémentaires. Plus particulièrement, ces discussions aident les membres de l'équipe affectés à la mission à examiner les informations contradictoires qui peuvent ressortir de leur propre connaissance de la nature et des circonstances de l'entité ;
- Fournissent une base à partir de laquelle les membres de l'équipe affectés à la mission communiquent et partagent de nouvelles informations recueillies tout au long de l'audit et qui peuvent affecter l'évaluation des risques d'anomalies significatives ou les procédures d'audit mises en œuvre pour répondre à ces risques.

La norme ISA 240²⁶ requiert que les discussions de l'équipe affectée à la mission visent tout particulièrement à déterminer comment et dans quels domaines les états financiers de l'entité sont susceptibles de comporter des anomalies significatives résultant de fraudes, et comment une fraude aurait pu être perpétrée.

A43. L'esprit critique est indispensable à une évaluation appropriée des éléments probants et, même dans le cas d'audits récurrents, la tenue de discussions approfondies et ouvertes entre les membres de l'équipe affectés à la mission peut améliorer l'identification et l'évaluation des risques d'anomalies significatives. De tels entretiens peuvent aussi aider l'auditeur à cerner des aspects précis de l'audit pour lesquels l'exercice de l'esprit critique pourrait s'avérer particulièrement important, et impliquer les membres plus expérimentés de l'équipe affectés à la mission possédant les compétences nécessaires à prendre part à la mise en œuvre des procédures d'audit se rapportant à ces domaines.

Application proportionnée

A44. Lorsque la mission est réalisée par une seule personne (comme un professionnel exerçant à titre individuel) et que, par conséquent, il ne peut y avoir de discussions entre les membres de l'équipe affectés à la mission, la prise en compte des points mentionnés aux paragraphes A42 et A46 peut néanmoins aider l'auditeur à identifier les domaines dans lesquels des risques d'anomalies significatives peuvent exister.

²⁶ Norme ISA 240, paragraphe 16.

A45. Lorsque l'équipe affectée à la mission compte un grand nombre de personnes, comme dans un audit d'états financiers de groupe (pour une entité à établissements multiples, par exemple), il n'est pas toujours nécessaire ou commode que tous ses membres participent en même temps aux discussions. Il n'est pas non plus nécessaire qu'ils soient tous informés de chacune des décisions prises au cours des discussions. L'associé responsable de la mission peut s'entretenir de certains points avec les membres clés de l'équipe, y compris, s'il le juge approprié, les membres possédant des compétences ou des connaissances particulières et les responsables des audits des composantes du groupe, et déléguer à d'autres les entretiens avec les autres membres de l'équipe, compte tenu de l'étendue de la communication jugée nécessaire. Un plan de communication approuvé par l'associé responsable de la mission peut s'avérer utile.

Entretiens au sujet des informations à fournir selon le référentiel comptable applicable

A46. Lors des entretiens entre les membres de l'équipe affectée à la mission, la prise en compte des obligations d'information du référentiel comptable applicable permet d'identifier au début de l'audit les domaines dans lesquels des risques d'anomalies significatives relatives aux informations fournies peuvent exister, même dans les cas où ce référentiel ne comporte que des obligations d'information simplifiées. L'équipe affectée à la mission peut discuter des points suivants :

- Des modifications des exigences en matière de l'élaboration de l'information financière qui peuvent donner lieu à d'importantes obligations d'information à fournir, que ces informations soient nouvelles ou modifiées ;
- Des changements dans l'environnement de l'entité, dans sa situation financière, ou dans ses activités, qui peuvent donner lieu à d'importantes obligations d'information à fournir, nouvelles ou modifiées, par exemple, un important regroupement d'entreprises survenu au cours de la période faisant l'objet de l'audit ;
- des informations à fournir pour lesquelles l'obtention d'éléments probants suffisants et appropriés par l'auditeur a peut-être été difficile dans le passé, et ;
- des informations à fournir sur des questions complexes, y compris celles sur lesquelles la direction doit porter des jugements importants au sujet des informations qu'il convient de communiquer.

Considérations propres aux entités du secteur public

A47. Lors des entretiens entre les membres de l'équipe affectés à la mission, les auditeurs d'entités du secteur public peuvent aussi discuter d'objectifs généraux supplémentaires liés au mandat d'audit ou aux obligations auxquelles doivent se conformer les entités du secteur public, et des risques se rattachant à ces objectifs.

Prise de connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité (Voir par. 19–27)

Les annexes 1 à 6 présentent des éléments à prendre en considération lors de la prise de connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité.
--

Prise de connaissance requise (Voir par. 19–27)

A48. La prise de connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité est un processus dynamique et itératif de collecte, de mise à jour et d'analyse d'informations qui se poursuit tout au long de l'audit. Par conséquent, les attentes de l'auditeur peuvent varier en fonction des nouvelles informations obtenues.

A49. La connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable peut également aider l'auditeur à définir des attentes initiales concernant les flux d'opérations, aux soldes de comptes et aux informations à fournir qui peuvent constituer des flux d'opérations importants, des soldes de comptes importants et des informations à fournir importantes. Les attentes relatives aux flux d'opérations importants, aux soldes de comptes importants et aux informations à fournir importantes forment la base pour définir l'étendue de sa connaissance du système d'information de l'entité.

Raisons pour lesquelles la prise de connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable est exigée (Voir par. 19–20)

A50. La connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable aide l'auditeur, d'une part, à comprendre les événements et les situations qui sont pertinents pour l'entité et, d'autre part, à déterminer la façon dont les facteurs de risque inhérent influent sur la possibilité que les assertions comportent des anomalies et la mesure dans laquelle ils influent sur cette possibilité, dans le cadre de la préparation des états financiers conformément au référentiel comptable applicable. Ainsi, l'auditeur dispose d'un cadre de référence pour l'identification et l'évaluation des risques d'anomalies significatives. Ce cadre de référence lui est également utile pour planifier l'audit et pour exercer son jugement professionnel et son esprit critique tout au long de la mission, notamment lorsqu'il :

- identifie et évalue les risques d'anomalies significatives dans les états financiers conformément à la norme ISA 315 (révisée en 2019) ou aux autres normes pertinentes (en ce qui concerne, par exemple, les risques de fraude, conformément à la norme ISA 240, ou dans le cadre de l'identification ou de l'évaluation des risques liés aux estimations comptables, conformément à la norme ISA 540 (révisée)) ;
- met en œuvre des procédures visant à faciliter l'identification des cas de non-conformité aux textes législatifs et réglementaires qui pourraient avoir une incidence significative sur les états financiers, conformément à la norme ISA 250 (révisée)²⁷ ;
- évalue si les états financiers fournissent des informations adéquates, conformément à la norme ISA 700 (révisée)²⁸ ;
- détermine un seuil de signification ou un seuil de planification, conformément à la norme ISA 320²⁹ ;
- évalue le caractère approprié du choix et de l'application des méthodes comptables et le caractère adéquat des informations fournies dans les états financiers.

A51. La connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable aide également l'auditeur à déterminer comment planifier et mettre en œuvre des procédures d'audit complémentaires, notamment lorsqu'il :

- définit des attentes qui seront utilisées lors de la mise en œuvre des procédures analytiques, conformément à la norme ISA 520³⁰ ;
- conçoit et met en œuvre des procédures d'audit complémentaires en vue de recueillir des éléments probants suffisants et appropriés, conformément à la norme ISA 330 ;
- évalue le caractère suffisant et approprié des éléments probants recueillis (en ce qui concerne, par exemple, les hypothèses retenues par la direction ou les déclarations orales et écrites faites par celle-ci).

²⁷ Norme ISA 250 (révisée), *Prise en compte des textes légaux et réglementaires dans un audit d'états financiers*, paragraphe 14

²⁸ Norme ISA 700 (révisée), *Opinion et rapport sur des états financiers*, par. 13 (e)

²⁹ Norme ISA 320, *Caractère significatif dans la planification et la réalisation d'un audit*, paragraphes 10 et 11

³⁰ Norme ISA 520, paragraphe 5

Application proportionnée

A52. La nature et l'étendue de la connaissance requise relèvent du jugement professionnel de l'auditeur et varient en fonction de la nature et des circonstances de chaque entité, dont :

- la taille et la complexité de l'entité, y compris son environnement informatique ;
- l'expérience passée de l'auditeur auprès de l'entité ;
- la nature des systèmes et processus de l'entité, y compris la mesure dans laquelle ils sont formalisés ;
- la nature de la documentation de l'entité et la forme sous laquelle elle se présente.

A53. Les procédures d'évaluation des risques que met en œuvre l'auditeur pour acquérir la connaissance requise dans le cadre de l'audit peuvent être moins étendues pour une entité peu complexe et, à l'inverse, plus poussées pour une entité plus complexe. Le niveau de connaissance que l'auditeur est tenu d'acquérir pour réaliser la mission devrait être moins élevé que celui dont la direction a besoin pour gérer l'entité.

A54. Certains référentiels comptables permettent aux petites entités de fournir, dans leurs états financiers, des informations dont le niveau de complexité et de détail est moins élevé. Cependant, cela ne dégage en rien l'auditeur de l'obligation de prendre connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable, dans le contexte propre à l'entité.

A55. L'utilisation que fait l'entité de l'informatique de même que la nature et l'étendue des changements survenus dans l'environnement informatique peuvent aussi avoir une incidence sur les compétences spécialisées nécessaires pour permettre la prise de connaissance requise.

L'entité et son environnement (Voir par. 19(a))

Structure organisationnelle, détention du capital, structures de gouvernance et modèle économique (Voir par. 19(a)(i))

Structure organisationnelle et détention du capital

A56. La connaissance de la structure organisationnelle et de la détention du capital de l'entité peut éclairer l'auditeur sur :

- la complexité de la structure de l'entité ;

Exemple :

L'entité peut être une entité unique ou, au contraire, présenter une structure comportant des filiales, des divisions ou d'autres composantes dans de multiples localisations. Par ailleurs, la structure juridique peut ne pas correspondre à la structure opérationnelle. Les structures complexes font souvent intervenir des facteurs qui peuvent accroître la possibilité de risques d'anomalies significatives. De telles questions peuvent viser la comptabilisation adéquate des écarts d'acquisition (goodwills), des co-entreprises, des participations ou des entités ad hoc et si des informations adéquates ont été fournies à leur sujet dans les états financiers.

- la détention du capital ainsi que les relations entre les propriétaires et d'autres personnes ou entités, y compris des parties liées. Cette connaissance peut aider l'auditeur à déterminer si les opérations avec des parties liées ont été correctement identifiées, comptabilisées et communiquées dans les états financiers³¹ ;

³¹ La norme ISA 550 contient des exigences et des indications sur les éléments à prendre en compte par l'auditeur en ce qui concerne les parties liées.

- la distinction entre les propriétaires, les personnes constituant le gouvernement d'entreprise et la direction ;

Exemple :

Dans les entités peu complexes, les propriétaires peuvent participer à la gestion et que la distinction entre les propriétaires, les personnes constituant le gouvernement d'entreprise et la direction soit minimale, voire inexistante; dans d'autres entités, notamment celles qui sont cotées, cette distinction peut être très claire³².

- La structure et la complexité de l'environnement informatique de l'entité.

Exemples :

Une entité peut :

- avoir un environnement informatique complexe résultant de l'accumulation de plusieurs anciens systèmes utilisés dans différents secteurs d'activité sans être bien intégrés ;
- confier la gestion de certains aspects de son environnement informatique à des fournisseurs de services internes ou externes (par exemple, en ayant recours aux services d'hébergement de tiers pour son environnement informatique ou en confiant la gestion de ses processus informatiques au centre de services partagés du groupe auquel elle appartient).

Outils et techniques automatisés

A57. Lorsque l'auditeur met en œuvre des procédures en vue de prendre connaissance du système d'information, il peut se servir d'outils et de techniques automatisés pour comprendre le flux des opérations et le processus de traitement. Grâce à ces procédures, l'auditeur peut être en mesure d'obtenir des informations sur la structure organisationnelle de l'entité ou sur les parties avec lesquelles l'entité exerce ses activités (par exemple, ses fournisseurs, ses clients et ses parties liées).

Considérations propres aux entités du secteur public

A58. Dans le secteur public, le mode de propriété de l'entité peut ne pas être aussi pertinent que dans le secteur privé car les processus politiques peuvent faire en sorte que des décisions qui concernent l'entité sont prises à l'extérieur de celle-ci et échappent donc au contrôle de la direction. Il pourrait être utile de comprendre, entre autres, la capacité de l'entité à prendre des décisions unilatérales, et la capacité d'autres entités du secteur public à contrôler ou à influencer le mandat et l'orientation stratégique de l'entité.

Exemple :

Une entité du secteur public peut être assujettie à des textes législatifs ou à d'autres directives de la part des autorités lui imposant d'obtenir l'approbation de parties externes à l'égard de sa stratégie et de ses objectifs avant leur mise en œuvre. Par conséquent, la connaissance de la structure juridique de l'entité peut notamment porter sur les textes législatifs et réglementaires applicables et sur le type d'entité dont il est question (ministère, administration, agence ou autre).

Gouvernance

Raisons pour lesquelles l'auditeur acquiert une connaissance de la gouvernance

A59. La connaissance de la gouvernance peut aider l'auditeur à connaître la capacité de l'entité à exercer une surveillance adéquate sur son système de contrôle interne. Elle peut aussi l'aider à relever des

³² Les paragraphes A1 et A2 de la norme ISA 260 (révisée) fournissent des indications sur l'identification des responsables de la gouvernance et précisent que, dans certains cas, une partie ou la totalité des responsables de la gouvernance peuvent participer à la gestion de l'entité.

déficiences, lesquelles peuvent indiquer une possibilité accrue de risques d'anomalies significatives dans les états financiers de l'entité.

Connaissance de la gouvernance de l'entité

A60. L'auditeur peut considérer les sujets suivants pour prendre connaissance de la gouvernance de l'entité:

- si une partie ou la totalité des personnes constituant le gouvernement d'entreprise participent à la gestion de l'entité ;
- s'il existe un conseil non exécutif (et, le cas échéant, comment ce conseil est distinct de la direction opérationnelle) ;
- si les personnes constituant le gouvernement d'entreprise occupent des postes qui font partie intégrante de la structure juridique de l'entité, comme des postes d'administrateurs ;
- si les personnes constituant le gouvernement d'entreprise sont réunis en sous-groupes, comme un comité d'audit (et, le cas échéant, quelles sont les responsabilités de chacun de ces sous-groupes) ;
- quelles sont les responsabilités des personnes constituant le gouvernement d'entreprise en matière de surveillance de l'information financière, notamment en ce qui concerne l'approbation des états financiers.

Modèle économique de l'entité

L'Annexe 1 fournit d'autres exemples d'éléments à prendre en considération pour prendre connaissance de l'entité et de son modèle économique, de même que des aspects particuliers à considérer lors de l'audit d'une entité ad hoc.

Raisons pour lesquelles l'auditeur acquiert une connaissance du modèle économique de l'entité

A61. La connaissance des objectifs, de la stratégie et du modèle économique de l'entité aide l'auditeur à comprendre l'aspect stratégique de l'entité ainsi que les risques liés à l'activité qu'elle prend et ceux auxquels elle est exposée. Comprendre les risques liés à l'activité ayant une incidence sur les états financiers aide l'auditeur à identifier les risques d'anomalies significatives, car la plupart des risques liés à l'activité finissent par avoir des conséquences financières et, donc, une incidence sur les états financiers.

Exemples :

Un modèle économique de l'entité peut reposer sur le recours à l'informatique de différentes façons :

- l'entité vend des chaussures dans un magasin et utilise un système de gestion de stock sophistiqué et de points de vente pour comptabiliser les ventes ;
- l'entité vend des chaussures en ligne, et tout le processus de vente, y compris le déclenchement de l'opération à partir d'un site Web, se déroule dans un environnement informatique.

Ces modèles économiques étant sensiblement différents, les risques liés à l'activité découlant de chacun le seront eux aussi, même si les deux entités vendent des chaussures.

Connaissance du modèle économique de l'entité

A62. Tous les aspects du modèle économique ne sont pas pertinents pour la connaissance de l'auditeur. Bien que l'incluant, les risques liés à l'activité sont plus larges que les risques que les états financiers comportent des anomalies significatives. ceux-ci. L'auditeur n'est pas tenu de prendre connaissance ou d'identifier tous les risques liés à l'activité, car ceux-ci ne donnent pas tous lieu à des risques d'anomalies significatives.

A63. Les risques liés à l'activité pouvant accroître la possibilité de risques d'anomalies significatives peuvent découler :

- d'objectifs ou de stratégies inappropriés, d'un manque d'efficacité dans la mise en œuvre des stratégies, ou encore de facteurs tels que le changement ou la complexité ;
- du fait de ne pas reconnaître le besoin de changement et les risques liés à l'activité qui en découlent, par exemple :
 - l'échec possible du développement de nouveaux produits ou services,
 - un marché qui, malgré le développement réussi d'un produit ou service, est insuffisant pour ce produit ou service,
 - des défauts d'un produit ou service susceptibles d'engager la responsabilité légale de l'entité ou d'entraîner un risque de réputation ;
- d'incitations ou de pressions qui amènent la direction à introduire un biais, intentionnel ou non, et qui, de ce fait, ont une incidence sur le caractère raisonnable des hypothèses importantes et sur les attentes de la direction et des personnes constituant le gouvernement d'entreprise.

A64. La liste suivante comprend des exemples de points que l'auditeur peut prendre en considération lors de sa prise de connaissance des objectifs, des stratégies et des risques liés à l'activité qui peuvent engendrer un risque que les états financiers comportent des anomalies significatives:

- Développements du secteur d'activité, comme le manque de personnel ou l'expertise dont elle a besoin pour faire face aux changements dans le secteur ;
- Nouveaux produits et services pouvant donner lieu à une responsabilité accrue du fabricant ;
- Développement de l'activité de l'entité, lorsque la demande n'a pas été correctement estimée ;
- Nouvelles exigences en matière comptables dont l'application est incomplète ou incorrecte ;
- Exigences réglementaires pouvant donner lieu à une exposition accrue à des actions en justice ;
- Besoins de refinancement présents , comme la perte de financements due à l'incapacité de l'entité à tenir ses engagements ;
- Utilisation de l'informatique comme la mise en œuvre d'un nouveau système informatique ayant une incidence tant sur les activités que sur l'information financière de l'entité ;
- Effets de la mise en œuvre d'une stratégie, en particulier les effets qui pourraient induire de nouvelles exigences comptables.

A65. Généralement, la direction identifie les risques liés à l'activité et définit des approches pour y répondre. Une telle procédure d'évaluation des risques fait partie du système de contrôle interne de l'entité et est abordée aux paragraphes 22 et A109–A113.

Considérations propres aux entités du secteur public

A66. Des entités exerçant leurs activités dans le secteur public peuvent créer et délivrer de la valeur de manière différente que les entités qui créent de la valeur pour leurs propriétaires bien qu'elles aient quand même un « modèle économique » visant un objectif particulier. Des exemples d'éléments que l'auditeur d'une entité du secteur public peut prendre en considération pour prendre connaissance du modèle économique incluent :

- la connaissance des activités gouvernementales pertinentes et des programmes y afférents ;
- les objectifs et les stratégies des programmes, y compris les questions relatives aux politiques publiques.

A67. Lorsque les audits portent sur des entités du secteur public, les « objectifs de la direction » peuvent être influencés par l'obligation de rendre des comptes au public et que certains de ces objectifs découlent de la législation, la réglementation ou les instructions d'une autre autorité .

Facteurs relatifs au secteur d'activité, facteurs réglementaires et autres facteurs externes (Voir sous-paragraphe 19(a)(ii))

Facteurs relatifs au secteur d'activité

A68. Les facteurs relatifs au secteur d'activité concernent les conditions sectorielles telles que le marché et la concurrence, les relations avec les clients et les fournisseurs et les développements technologiques. Les domaines que l'auditeur peut prendre en compte comprennent :

- Le marché et la concurrence, y compris la demande, la capacité de production et la concurrence sur les prix ;
- l'activité cyclique ou saisonnière ;
- la technologie des produits fabriqués par l'entité ;
- l'approvisionnement énergétique et son coût.

A69. Le secteur d'activité dans lequel l'entité opère peut générer des risques spécifiques d'anomalies significatives résultant de la nature des activités ou du niveau de réglementation.

Exemple :

Dans le secteur de la construction, certains contrats à long terme peuvent nécessiter des estimations importantes des produits et des charges qui donnent lieu à des risques d'anomalies significatives. Dans ce cas, il importe que l'équipe affectée à la mission compte des membres disposant de connaissances et d'expérience pertinentes et suffisantes³³.

Facteurs réglementaires

A70. Les facteurs réglementaires pertinents visent l'environnement réglementaire. Ce dernier englobe, parmi d'autres aspects, le référentiel comptable applicable, ainsi que le contexte légal et politique, et tout changement les concernant. Les sujets que l'auditeur peut prendre en compte comprennent :

- le cadre réglementaire propre à un secteur d'activité réglementé, tel que des exigences prudentielles, incluant les obligations d'informations à fournir les concernant ;
- le cadre législatif et réglementaire qui affecte de manière importante les opérations de l'entité, par exemple en matière de réglementation et du droit du travail ;
- le cadre législatif et réglementaire en matière de fiscalité ;
- Les politiques gouvernementales affectant la conduite des affaires courantes de l'entité, telles que la politique monétaire, y compris le contrôle des changes, la politique budgétaire, les incitations financières (par exemple gouvernementales), ainsi que la politique de tarification ou de restrictions commerciales ;
- Les exigences environnementales affectant le secteur d'activité et les opérations de l'entité.

A71. La norme ISA 250 (révisée) contient des diligences portant spécifiquement sur le cadre légal et réglementaire applicable à l'entité et à son secteur d'activité³⁴.

Considérations propres aux entités du secteur public

A72. Lorsque l'audit porte sur une entité du secteur public, des textes légaux ou réglementaires particuliers peuvent avoir une incidence sur le fonctionnement de l'entité. Il peut être essentiel d'en tenir compte lors de la prise de connaissance de l'entité et de son environnement.

³³ Norme ISA 220 (révisée), paragraphe 14.

³⁴ Norme ISA 250 (révisée), paragraphe 13.

Autres facteurs externes

A73. D'autres facteurs externes affectant l'entité que l'auditeur peut prendre en considération, comprennent les conditions du niveau général de l'activité économique, les taux d'intérêts et les possibilités de financement, l'inflation ou la réévaluation monétaire.

Mesures utilisées par la direction afin d'évaluer la performance financière de l'entité (Voir par. 19(a)(iii))

Raisons pour lesquelles l'auditeur acquiert une connaissance des mesures utilisées par la direction

A74. La connaissance des mesures de l'entité aide l'auditeur à déterminer si l'utilisation de ces mesures, par l'entité ou par des parties externes, fait en sorte que l'entité subit des pressions qui la poussent à atteindre des objectifs de performance. De telles pressions peuvent amener la direction à agir d'une manière qui augmente la possibilité d'anomalies résultant de biais introduits par la direction ou provenant de fraudes ; par exemple, elles peuvent l'inciter à prendre des mesures pour améliorer la performance opérationnelle ou à présenter intentionnellement des états financiers mensongers (les diligences et les indications relatives aux risques de fraude sont détaillées dans la norme ISA 240).

A75. Les mesures peuvent par ailleurs renseigner l'auditeur sur la probabilité que les informations correspondantes dans les états financiers présentent des risques d'anomalies significatives. Par exemple, les mesures de performance peuvent indiquer que l'entité bénéficie d'une croissance rapide ou d'une rentabilité anormales par rapport à d'autres entités dans le même secteur d'activité.

Mesures utilisées par la direction

A76. Généralement, la direction et d'autres personnes mesureront et analyseront les sujets qu'elles considèrent d'importance. Des demandes d'informations auprès de la direction peuvent révéler que celle-ci s'appuie sur certains indicateurs clés, publiés ou non, pour évaluer la performance financière et mener des actions. En pareil cas, l'auditeur peut considérer l'information utilisée par l'entité à des fins de gestion afin de d'identifier les mesures de performance pertinentes, tant internes qu'externes.. Si de telles demandes indiquent l'absence d'outils de mesure ou d'analyse de la performance, il peut alors exister un risque plus élevé d'anomalies non détectées et non corrigées.

A77. Des exemples d'indicateurs clés utilisés pour évaluer la performance financière peuvent être les suivants :

- Indicateurs-clés de performance (financiers et non financiers), ratios-clés, tendances et statistiques opérationnelles ;
- Analyses comparatives de performance financière sur plusieurs périodes ;
- Budgets, prévisions, analyses de variations, informations sectorielles et rapports de performance par division, par département ou par autre niveau ;
- Évaluation de la performance des membres du personnel et des politiques de rémunération incitatives ;
- Comparaison de la performance de l'entité avec celle de ses concurrents.

Application proportionnée (Voir par. 19(a)(iii))

A78. Les procédures que l'auditeur met en œuvre pour comprendre les mesures de l'entité peuvent varier selon la taille ou la complexité de l'entité et selon la mesure dans laquelle les propriétaires ou les personnes constituant le gouvernement d'entreprise participent à sa gestion.

Exemples :

- Certaines entités peu complexes peuvent se voir imposer des conditions d'emprunt bancaire (clauses restrictives) se rapportant à des mesures de performance précises en lien avec la performance ou la situation financière de l'entité (par exemple, le maintien d'un certain montant de fonds de roulement). La connaissance des mesures de performance utilisées par la banque peut aider l'auditeur à identifier les domaines où la possibilité de risques d'anomalies significatives est accrue.
- Pour certaines entités dont la nature et les circonstances sont plus complexes, comme celles qui exercent leurs activités dans les secteurs des banques ou de l'assurance, la performance ou la situation financière peuvent être évaluées au regard d'exigences réglementaires (telles que les ratios de fonds propres et de liquidité requis). La connaissance de ces mesures de performance peut aider l'auditeur à identifier les domaines où la possibilité de risques d'anomalies significatives est accrue.

Autres éléments à prendre en considération

A79. Des parties externes peuvent également examiner et analyser la performance financière de l'entité, notamment lorsque l'information financière la concernant est accessible au public. Afin de mieux connaître les activités de l'entité ou déceler des informations contradictoires, l'auditeur peut aussi prendre en considération les informations publiques, dont celles qui proviennent :

- des analystes ou des agences de notation ;
- de la presse ou d'autres médias, y compris les médias sociaux ;
- des autorités fiscales ;
- des autorités de contrôle ;
- des syndicats ;
- des bailleurs de fonds.

Il est souvent possible d'obtenir de telles informations financières auprès de l'entité auditée.

A80. La mesure et l'analyse de la performance financière ne sont pas de même nature que le suivi du système de contrôle interne (traité comme une composante du système de contrôle interne aux paragraphes A114–A122), bien que leurs objectifs puissent se recouper :

- La mesure et l'analyse de la performance ont pour but de déterminer si la performance opérationnelle répond aux objectifs fixés par la direction (ou des tiers) ;
- Par opposition, le suivi du système de contrôle interne vise à surveiller le fonctionnement effectif des contrôles, dont ceux qui concernent la mesure et l'analyse, par la direction, de la performance financière.

Dans certains cas cependant, les indicateurs de performance fournissent aussi des informations qui permettent à la direction d'identifier des faiblesses de contrôle.

Considérations propres aux entités du secteur public

A81. En plus de prendre en considération les mesures pertinentes dont se sert l'entité du secteur public pour évaluer sa performance financière, les auditeurs de telles entités peuvent également tenir compte d'informations non financières, telles que les résultats atteints au profit du public (par exemple, le nombre de bénéficiaires d'un programme en particulier).

Référentiel comptable applicable (Voir par. 19(b))

Connaissance du référentiel comptable applicable et des méthodes comptables retenues par l'entité

A82. Des éléments que l'auditeur peut prendre en considération pour acquérir la connaissance du référentiel comptable applicable et de la manière dont il s'applique au regard de la nature et des circonstances de l'entité et de son environnement incluent :

- les pratiques d'élaboration de l'information financière de l'entité se rapportant au référentiel comptable applicable :
 - principes comptables et pratiques sectorielles spécifiques, y compris les flux d'opérations, les soldes de comptes et les informations à fournir les concernant dans les états financiers importants du secteur (par exemple, les prêts ou emprunts dans les banques, ou la recherche et le développement dans l'industrie pharmaceutique),
 - reconnaissance des produits,
 - traitement comptable des instruments financiers, y compris les pertes de crédit s'y rattachant,
 - actifs et passifs en monnaies étrangères et opérations en devises ;
 - Comptabilisation des opérations inhabituelles ou complexes, y compris celles dans des domaines controversés ou nouveaux (par exemple, comptabilisation des cryptomonnaies) ;
- La connaissance des choix des politiques comptables par l'entité et leur application et, le cas échéant, des changements dans celles-ci et des raisons ayant motivé ces changements, peut comprendre des sujets tels que :
 - Les méthodes utilisées par l'entité pour reconnaître, mesurer, présenter des opérations importantes et inhabituelles ainsi que la fourniture d'informations à leur sujet,
 - L'impact de politiques comptables importantes appliquées dans des domaines controversés ou nouveaux pour lesquels il n'existe pas de règles édictées ou de consensus,
 - Les changements dans l'environnement, tels que des modifications apportées au référentiel comptable applicable ou une réforme fiscale, qui nécessitent un changement des méthodes comptables retenues par l'entité,
 - Les normes et les textes législatifs et réglementaires en matière d'information financière qui sont nouvellement applicables à l'entité et la façon dont l'entité les adoptera.

A83. La prise de connaissance de l'entité et de son environnement peut aider l'auditeur lorsqu'il détermine les domaines où des changements dans l'information financière de l'entité (par rapport aux exercices précédents, par exemple) peuvent être attendus.

Exemple :

Si une entité a participé à un important regroupement d'entreprises au cours de la période, l'auditeur s'attendra probablement à ce qu'il y ait des changements dans les flux d'opérations, les soldes de comptes et les informations à fournir touchés par ce regroupement. Dans d'autres cas, en l'absence de changement important dans le référentiel comptable applicable au cours de la période, la connaissance acquise par l'auditeur aidera celui-ci à s'assurer que la connaissance qu'il a acquise au cours de la période précédente demeure applicable.

Considérations propres aux entités du secteur public

A84. Dans le secteur public, c'est le cadre législatif et réglementaire propre à chaque juridiction ou à la zone géographique qui détermine le référentiel comptable applicable, notamment l'utilisation par l'entité, au regard de sa nature, des circonstances et de son environnement, d'une comptabilité

d'engagement ou d'une comptabilité de trésorerie, conformément aux Normes comptables internationales du secteur public, ou d'une méthode hybride.

Manière dont les facteurs de risque inhérent influent sur la possibilité que les assertions portant sur des flux d'opérations, des soldes de comptes ou des informations à fournir comportent des anomalies (Voir par. 19(c))

L'**Annexe 2** présente des exemples d'événements et de situations pouvant donner lieu à des risques d'anomalies significatives, classés selon la catégorie de facteurs de risque inhérent.

Raisons pour lesquelles l'auditeur acquiert une connaissance des facteurs de risque inhérent dans le cadre de la prise de connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable

- A85. La connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable aide l'auditeur à reconnaître les événements ou situations qui présentent des facteurs de risque inhérent, c'est-à-dire des caractéristiques pouvant avoir une incidence sur la possibilité que les assertions portant sur des flux d'opérations, des soldes de comptes ou des informations à fournir comportent des anomalies. Ces facteurs de risque inhérent peuvent avoir une incidence sur la possibilité que les assertions comportent des anomalies, en influant sur la probabilité qu'une anomalie se produise et sur l'ampleur qu'elle pourrait prendre. Ainsi, la prise de connaissance de la façon dont les facteurs de risque inhérent influent sur la possibilité que les assertions comportent des anomalies peut aider l'auditeur à acquérir une première compréhension de la probabilité ou de l'ampleur des anomalies, laquelle lui sera utile pour identifier les risques d'anomalies significatives au niveau des assertions conformément au paragraphe 28(b). Quant à la connaissance de la mesure dans laquelle les facteurs de risque inhérent influent sur la possibilité d'anomalies significatives, elle peut aider l'auditeur à évaluer le risque inhérent, conformément au paragraphe 31(a). La connaissance des facteurs de risque inhérent aide aussi l'auditeur à concevoir et à mettre en œuvre des procédures d'audit complémentaires conformément à la norme ISA 330.
- A86. Les éléments probants recueillis par l'auditeur lorsqu'il met en œuvre d'autres procédures d'évaluation des risques ou des procédures d'audit complémentaires, ou lorsqu'il s'acquitte d'autres diligences contenues dans les normes ISA (voir les paragraphes A95, A103, A111, A121, A124 et A151), peuvent aussi influencer sur l'identification des risques d'anomalie significatives au niveau des assertions et sur l'évaluation du risque inhérent.

Incidence des facteurs de risque inhérent sur un flux d'opérations, un solde de compte ou une information à fournir

- A87. Plus il y a de changement ou d'incertitude concernant un flux d'opérations, un solde de compte ou une information à fournir, plus la complexité ou la subjectivité influent sur la possibilité que ce flux d'opérations, ce solde de compte ou cette information à fournir comporte une anomalie, car ces facteurs sont étroitement liés.

Exemple :

Si l'entité a basé une estimation comptable sur des hypothèses dont le choix nécessite une grande part de jugement, il est probable que la subjectivité et l'incertitude aient toutes deux une incidence sur la mesure de l'estimation comptable.

- A88. Plus la complexité ou la subjectivité influe sur la possibilité qu'un flux d'opérations, un solde de compte ou une information à fournir comporte une anomalie, plus il est nécessaire que l'auditeur fasse preuve d'esprit critique. En outre, la complexité, la subjectivité, le changement et l'incertitude sont des facteurs de risque inhérent qui, lorsqu'ils influent sur la possibilité qu'un flux d'opérations, un solde de compte ou une information à fournir comporte une anomalie, peuvent donner l'occasion

à la direction d'introduire un biais, intentionnel ou non, et accroître la possibilité d'anomalies résultant de biais introduits par la direction. L'interrelation entre les facteurs de risque inhérent a donc, au niveau des assertions, une incidence à la fois sur l'identification par l'auditeur des risques d'anomalies significatives et sur son évaluation du risque inhérent.

- A89. Des événements ou des situations qui peuvent avoir une incidence sur la possibilité d'anomalies résultant de biais introduits par la direction peuvent avoir également une incidence sur la possibilité d'anomalies résultant d'autres facteurs de risque de fraude. Par conséquent, il peut être pertinent que l'auditeur en tienne compte lorsque, conformément au paragraphe 24 de la norme ISA 240, il évalue si les informations qu'il a obtenues lors de la mise en œuvre des autres procédures d'évaluation des risques et des procédures liées indiquent la présence d'un ou de plusieurs facteurs de risque de fraude.

Prise de connaissance du système de contrôle interne de l'entité (Voir par. 21–27)

La nature du système de contrôle interne de l'entité et les limites inhérentes au contrôle interne sont traitées de façon plus détaillée à l'**Annexe 3**, qui contient également des explications supplémentaires sur les composantes du système de contrôle interne pour les besoins des normes ISA.

- A90. L'auditeur acquiert la connaissance du système de contrôle interne de l'entité au moyen des procédures d'évaluation des risques mise en œuvre pour connaître et évaluer chacune des composantes du système de contrôle interne, comme il est énoncé aux paragraphes 21–27.
- A91. Les composantes du système de contrôle interne de l'entité au sens de la présente norme ISA ne reflètent pas nécessairement la manière dont une entité conçoit, met en œuvre et suit son système de contrôle interne, ni la manière dont elle classifie les différentes composantes. Les entités peuvent employer une autre terminologie ou un cadre différent pour décrire les divers aspects de son système de contrôle interne. Les auditeurs peuvent faire de même dans le cadre de leur audit, à condition cependant de tenir compte de toutes les composantes du système de contrôle interne qui sont décrites dans la présente norme ISA.

Application proportionnée

- A92. La manière dont le système de contrôle interne de l'entité est conçu, mis en œuvre et suivi varie selon la taille et la complexité de celle-ci. Ainsi, il est possible que les entités peu complexes aient recours à des contrôles (c'est-à-dire à des politiques et à des procédures) plus simples et moins structurés pour atteindre leurs objectifs.

Considérations propres aux entités du secteur public

- A93. Les auditeurs d'entités du secteur public ont souvent des responsabilités supplémentaires concernant le contrôle interne, par exemple celles de produire un rapport sur le respect d'un code de bonnes pratiques prescrit ou sur le respect des budgets. Ils peuvent avoir également la responsabilité de produire un rapport sur la conformité à la législation, à la réglementation ou aux instructions d'une autorité. Leur prise en compte du système de contrôle interne peut donc être plus étendue et plus détaillée.

Recours à l'informatique dans les composantes du système de contrôle interne de l'entité

L'**Annexe 5** fournit des indications supplémentaires sur la connaissance du recours à l'informatique par l'entité dans les composantes du système de contrôle interne.

- A94. L'objectif général et l'étendue de l'audit restent les mêmes, que l'entité exerce ses activités dans un environnement principalement manuel, entièrement automatisé, ou composé à la fois d'éléments

manuels et d'éléments automatisés (c'est-à-dire des contrôles manuels et automatisés ans d'autres ressources sont utilisées dans le système de contrôle interne de l'entité).

Connaissance de la nature des composantes du système de contrôle interne de l'entité

A95. Lorsque l'auditeur évalue l'efficacité de la conception des contrôles et détermine s'ils ont été mis en œuvre (voir par. A175–A181), sa connaissance de chacune des composantes du système de contrôle interne de l'entité lui permet d'avoir une connaissance préliminaire de la manière dont l'entité identifie les risques liés à l'activité et y répond. Cette connaissance peut également influencer de diverses manières l'identification et l'évaluation par l'auditeur des risques d'anomalies significatives (voir par. A86). Elle aide l'auditeur à concevoir et à mettre en œuvre des procédures d'audit complémentaires, y compris s'il a l'intention de tester l'efficacité du fonctionnement des. Par exemple :

- La connaissance qu'acquiert l'auditeur des composantes « environnement de contrôle », « processus d'évaluation des risques par l'entité » et « processus de suivi du système de contrôle interne par l'entité » auront probablement plus d'influence sur l'identification et l'évaluation des risques d'anomalies significatives au niveau des états financiers.
- La connaissance qu'acquiert l'auditeur des composantes « système d'information et communications » et « mesures de contrôle » de l'entité auront probablement plus d'influence sur l'identification et l'évaluation des risques d'anomalies significatives au niveau des assertions.

Environnement de contrôle, processus d'évaluation des risques par l'entité et processus de suivi du système de contrôle interne par l'entité (Voir par. 21–24)

A96. Les contrôles des composantes « environnement de contrôle », « processus d'évaluation des risques par l'entité » et « processus de suivi du système de contrôle interne par l'entité » sont principalement des contrôles indirects (c'est-à-dire des contrôles qui ne sont pas assez précis pour prévenir ou pour détecter et corriger les anomalies au niveau des assertions, mais qui favorisent le fonctionnement d'autres contrôles et qui peuvent donc influencer indirectement sur la probabilité qu'une anomalie soit détectée ou prévenue en temps opportun). Toutefois, certains des contrôles qui font partie de ces composantes peuvent être des contrôles directs.

Raisons pour lesquelles l'auditeur doit acquérir une connaissance de l'environnement de contrôle, du processus d'évaluation des risques par l'entité et du processus de suivi du système de contrôle interne par l'entité

A97. L'environnement de contrôle constitue l'assise sur laquelle repose le fonctionnement des autres composantes du système de contrôle interne. L'environnement de contrôle ne peut directement prévenir, ni détecter et corriger, les anomalies. Il peut toutefois influencer sur l'efficacité des contrôles qui font partie des autres composantes du système de contrôle interne. De façon similaire, les processus d'évaluation des risques et de suivi du système de contrôle interne par l'entité sont eux aussi conçus pour contribuer au bon fonctionnement du système de contrôle interne dans son ensemble.

A98. Étant donné que ces composantes constituent l'assise sur laquelle repose le système de contrôle interne de l'entité, toute déficience de leur fonctionnement peut avoir des effets diffus sur la préparation des états financiers. Par conséquent, la connaissance et l'évaluation de ces composantes par l'auditeur ont une incidence sur son identification et son évaluation des risques d'anomalies significatives au niveau des états financiers, et peuvent également avoir une incidence sur l'identification et l'évaluation des risques d'anomalies significatives au niveau des assertions. Les risques d'anomalies significatives au niveau des états financiers ont une incidence sur la conception

de l'approche générale de l'auditeur, notamment – comme expliqué dans la norme ISA 330 – sur la nature, le calendrier et l'étendue de ses procédures complémentaires³⁵.

Prise de connaissance de l'environnement de contrôle (Voir par. 21)

Application proportionnée

A99. L'environnement de contrôle d'une entité peu complexe est généralement d'une nature différente de celle d'une entité plus complexe. Par exemple, les personnes constituant le gouvernement d'entreprise dans les entités peu complexes peuvent ne pas inclure un membre indépendant ou extérieur, et le rôle de gouvernance peut être assumé directement par le propriétaire-dirigeant lorsqu'il n'existe pas d'autres détenteurs du capital. Par conséquent, certaines considérations relatives à l'environnement de contrôle de l'entité peuvent être moins pertinentes ou ne s'appliquent pas.

A100. De plus, les éléments probants concernant les éléments de l'environnement de contrôle dans les entités peu complexes peuvent ne pas être disponibles sous forme de documents, en particulier lorsque la communication entre la direction et les autres membres du personnel est informelle, mais peuvent être tout de même suffisamment pertinents et fiables dans les circonstances.

Exemples :

- La structure organisationnelle d'une entité peu complexe est généralement plus simple et le nombre d'employés exerçant des fonctions liées à l'information financière sont peu nombreux.
- Si le rôle de gouvernance est assumé directement par le propriétaire-dirigeant, l'auditeur peut juger que l'indépendance des personnes constituant le gouvernement d'entreprise n'est pas une question pertinente.
- Les entités peu complexes pourraient ne pas avoir un code de conduite écrit mais, en lieu et place, développer une culture d'entreprise qui met l'accent sur l'importance de l'intégrité et d'un comportement éthique au travers de la communication orale et par l'exemple que donne la direction. Par conséquent, les comportements, la prise de conscience et les actions de la direction ou du propriétaire-dirigeant revêtent une importance particulière pour la connaissance par l'auditeur de l'environnement de contrôle d'une entité peu complexe.

Connaissance de l'environnement de contrôle (Voir par. 21 (a))

A101. Les éléments probants pertinents peuvent être recueillis à partir d'une combinaison de demandes d'informations et d'autres procédures d'évaluation des risques (c'est-à-dire celles visant à corroborer des informations avec l'observation ou la revue de documents).

A102. Pour prendre connaissance de la mesure dans laquelle la direction démontre de l'importance à l'intégrité et aux valeurs éthiques, l'auditeur peut procéder à des demandes d'informations auprès de la direction et du personnel et prendre en considération des informations provenant de sources externes afin :

- de se renseigner sur la manière dont la direction communique aux membres du personnel ses vues sur les bonnes pratiques des affaires et le comportement éthique ;
- d'inspecter le code de conduite écrit de la direction et d'observer si elle agit conformément à ce code.

Évaluation de l'environnement de contrôle (Voir par. 21 (b))

Raisons pour lesquelles l'auditeur évalue l'environnement de contrôle

³⁵ Norme ISA 330, paragraphes A1–A3.

A103. L'évaluation de l'environnement de contrôle – c'est-à-dire le fait d'évaluer de quelle manière l'entité démontre, par son comportement, qu'elle attache de l'importance à l'intégrité et aux valeurs éthiques, et si l'environnement de contrôle fournit une base appropriée sur laquelle peuvent s'appuyer les autres composantes du système de contrôle interne de l'entité, et si les déficiences du contrôle relevées nuisent aux autres composantes du système de contrôle interne – aide l'auditeur à identifier d'éventuels problèmes liés aux autres composantes du système de contrôle interne. En effet, l'environnement de contrôle sert d'assise aux autres composantes du système de contrôle interne de l'entité. Cette évaluation peut aussi aider l'auditeur à comprendre les risques auxquels l'entité est exposée et donc à identifier et à évaluer les risques d'anomalies significatives au niveau des états financiers et au niveau des assertions (voir par. A86).

Évaluation de l'environnement de contrôle par l'auditeur

A104. Pour évaluer l'environnement de contrôle, l'auditeur se fonde sur la connaissance qu'il a acquise conformément au paragraphe 21(a).

A105. Certaines entités peuvent être soumises à l'emprise d'une personne qui peut détenir à elle seule un fort pouvoir discrétionnaire. Les actions et l'attitude de cette personne peuvent alors avoir un effet diffus sur la culture de l'entité et, par conséquent, sur l'environnement de contrôle. Une telle incidence peut être positive ou négative.

Exemple :

L'intervention directe d'une seule personne peut être un facteur clé permettant à l'entité d'atteindre ses objectifs de croissance ou d'autres objectifs, et de contribuer de façon importante au fonctionnement efficace du système de contrôle interne. En revanche, une telle concentration des connaissances et des pouvoirs peut aussi conduire à une possibilité accrue d'anomalies résultant du contournement des contrôles par la direction.

A106. L'auditeur peut prendre en considération l'influence éventuelle de la philosophie et du style de gestion de la haute direction sur les différents éléments de l'environnement de contrôle, en tenant compte du rôle joué par les membres indépendants parmi les personnes constituant le gouvernement d'entreprise.

A107. Il est possible qu'un environnement de contrôle adéquat procure une base appropriée sur laquelle peut s'appuyer le système de contrôle interne et qu'il contribue à réduire le risque de fraude, mais cela ne veut pas dire qu'il s'agit nécessairement d'un effet de dissuasion efficace.

Exemple :

Des politiques et pratiques de ressources humaines visant à recruter du personnel compétent dans les domaines financiers, comptables et informatiques peuvent compenser le risque d'erreurs dans le traitement et l'enregistrement de l'information financière. Cependant, elles ne permettent pas nécessairement d'empêcher la haute direction de contourner les contrôles (par exemple, pour surévaluer les bénéfices).

A108. L'évaluation de l'environnement de contrôle par l'auditeur relative à l'utilisation de l'informatique par l'entité peut inclure, par exemple :

- la mesure dans laquelle la gouvernance informatique est adaptée à la nature et à la complexité de l'entité et de ses activités qui dépendent de l'informatique, en tenant compte notamment de la complexité et de la maturité de la plateforme ou de l'architecture technologique de l'entité et de la mesure dans laquelle le processus d'information financière de l'entité repose sur des applications informatiques ;
- la structure organisationnelle de gestion de l'informatique et les ressources allouées aux technologies de l'information (par exemple, si l'entité s'est dotée d'un environnement informatique approprié et si elle a procédé aux améliorations nécessaires, ou encore si elle

peut compter sur un nombre suffisant d'employés compétents, y compris dans les cas où l'entité utilise un logiciel disponible sur le marché peu ou pas modifié).

Prise de connaissance du processus d'évaluation des risques par l'entité (Voir par. 22–23)

Connaissance du processus d'évaluation des risques par l'entité (Voir par. 22(a))

A109. Comme précisé au paragraphe A62, tous les risques liés à l'activité ne donnent pas lieu à des risques d'anomalies significatives. Pour comprendre comment la direction et les personnes constituant le gouvernement d'entreprise ont identifié les risques liés à l'activité afférents à la préparation des états financiers et ont décidé des mesures à prendre pour y répondre, l'auditeur peut, par exemple, considérer comment la direction ou, selon ce qui convient, les personnes constituant le gouvernement d'entreprise ont :

- défini les objectifs de l'entité avec suffisamment de précision et de clarté pour permettre l'identification et l'évaluation des risques s'y rattachant ;
- identifié et analysé les risques liés à l'atteinte des objectifs de l'entité afin de disposer d'une base leur permettant de déterminer comment gérer ces risques ;
- tenu compte, dans leur examen des risques liés à l'atteinte des objectifs de l'entité, de la possibilité que des fraudes soient commises³⁶.

A110. L'auditeur peut considérer les conséquences de ces risques liés à l'activité sur la préparation des états financiers et sur d'autres aspects du système de contrôle interne de l'entité.

Évaluation du processus d'évaluation des risques par l'entité (Voir par. 22(b))

Raisons pour lesquelles l'auditeur évalue le caractère approprié du processus d'évaluation des risques par l'entité

A111. L'évaluation par l'auditeur du processus d'évaluation des risques par l'entité peut l'aider à comprendre les domaines dans lesquels l'entité a identifié la possible survenance de risques et la manière dont elle y a répondu. L'évaluation de la manière dont l'entité identifie les risques liés à l'activité auxquels elle est exposée, les évalue et y répond, aide l'auditeur à comprendre si l'identification et l'évaluation de ces risques, ainsi que les mesures prises pour y répondre, sont appropriées compte tenu de la nature et de la complexité de l'entité. Cette évaluation peut également aider l'auditeur à identifier et à évaluer les risques d'anomalies significatives au niveau des états financiers et au niveau des assertions (voir par. A86).

Évaluation du caractère approprié du processus d'évaluation des risques par l'entité (Voir par. 22(b))

A112. Afin d'évaluer le caractère approprié du processus d'évaluation des risques par l'entité l'auditeur se fonde sur la connaissance acquise conformément au paragraphe 22(a).

Application proportionnée

A113. La question de savoir si le processus d'évaluation des risques par l'entité est approprié aux circonstances de l'entité, compte tenu de la nature et de la complexité de celle-ci, relève du jugement professionnel de l'auditeur.

³⁶ Norme ISA 240, paragraphe 19.

Exemple :

Dans certaines entités peu complexes (notamment celles qui sont gérées par un propriétaire-dirigeant), une intervention directe de la direction ou du propriétaire-dirigeant peut constituer un processus d'évaluation des risques approprié (par exemple, il est possible que le dirigeant ou le propriétaire-dirigeant prenne régulièrement le temps de suivre les activités de la concurrence et les nouveautés sur le marché pour identifier les risques émergents liés à l'activité). Dans les entités de ce type, il arrive souvent que cette évaluation des risques ne soit pas formellement documentée, mais que des entretiens entre l'auditeur et la direction révèlent qu'en fait, celle-ci met en œuvre des procédures d'évaluation des risques.

Prise de connaissance du processus de suivi du système de contrôle interne par l'entité (Voir par. 24)

Application proportionnée

A114. Dans les entités peu complexes (notamment celles qui sont gérées par un propriétaire-dirigeant), la connaissance qu'acquiert l'auditeur en ce qui concerne le processus de suivi du système de contrôle interne par l'entité est souvent axée sur la façon dont la direction ou le propriétaire-dirigeant participe directement à l'exploitation, car il se peut qu'il n'y ait aucune autre activité de suivi.

Exemple :

La direction peut recevoir des plaintes de clients concernant des inexactitudes dans leurs relevés mensuels, et que le propriétaire-dirigeant prenne ainsi conscience de problèmes liés au moment où les paiements des clients sont comptablement enregistrés.

A115. Dans les entités qui n'ont pas de processus formalisé de suivi du système de contrôle interne, la connaissance du processus de suivi du système de contrôle interne peut inclure la connaissance des examens périodiques de l'information comptable par la direction conçus pour contribuer à prévenir ou détecter des anomalies.

Connaissance du processus de suivi du système de contrôle interne par l'entité (Voir par. 24 (a))

A116. Des aspects pouvant être pertinents pour l'auditeur afin de comprendre comment l'entité effectue le suivi de son système de contrôle interne incluent :

- la conception des activités de suivi (activités périodiques ou permanentes, par exemple) ;
- l'exécution et la fréquence des activités de suivi ;
- l'évaluation en temps opportun des résultats des activités de suivi aux fins de l'évaluation de l'efficacité des contrôles ;
- la manière dont l'entité a pris des mesures correctives appropriées pour corriger les déficiences relevées, y compris ce qui a été fait pour communiquer ces déficiences en temps opportun aux personnes chargées de prendre des mesures correctives.

A117. L'auditeur peut aussi prendre en considération la manière dont s'effectue, dans le processus de suivi du système de contrôle interne par l'entité, le suivi des contrôles du traitement de l'information recourant à l'informatique, tels que :

- les contrôles de suivi d'environnements informatiques complexes qui visent :
 - soit à évaluer l'efficacité permanente de la conception des contrôles du traitement de l'information et à modifier ces contrôles, au besoin, pour tenir compte de changements de circonstances,
 - soit à évaluer l'efficacité du fonctionnement des contrôles du traitement de l'information ;
- les contrôles de suivi des autorisations se rapportant aux contrôles du traitement de l'information qui sont automatisés et qui assurent la séparation des tâches ;

- les contrôles de suivi de l'identification et de la correction des erreurs ou des déficiences de contrôle liées à l'automatisation du processus d'information financière.

Connaissance de la fonction d'audit interne de l'entité (Voir par. 24 (a)(ii))

L'**Annexe 4** fournit d'autres exemples d'éléments à prendre en considération pour prendre connaissance de la fonction d'audit interne de l'entité.

A118. Les demandes d'informations adressées aux personnes appropriées au sein de la fonction d'audit interne aident l'auditeur à prendre connaissance de la nature des responsabilités de la fonction d'audit interne. Si l'auditeur détermine que les responsabilités de la fonction ont un rapport avec l'information financière de l'entité, il peut acquérir une meilleure connaissance des activités qui ont été ou qui seront réalisées par la fonction d'audit interne en examinant, le cas échéant, le plan d'audit élaboré par celle-ci pour la période et en s'entretenant de ce plan avec les personnes appropriées au sein de la fonction. Cette connaissance ainsi que les informations obtenues grâce aux demandes d'informations peuvent également fournir des informations qui sont directement pertinentes pour l'identification et l'évaluation des risques d'anomalies significatives par l'auditeur. Si, compte tenu de la connaissance préliminaire qu'il a acquise de la fonction d'audit interne, l'auditeur compte s'appuyer sur les travaux de la fonction d'audit interne pour modifier la nature ou le calendrier des procédures d'audit à mettre en œuvre ou pour en réduire l'étendue, la norme ISA 610 (révisée en 2013)³⁷ s'applique.

Autres sources d'informations utilisées dans le cadre du processus de suivi du système de contrôle interne par l'entité

Connaissance des sources d'informations (Voir par. 24(b))

A119. Les activités de suivi effectuées par la direction peuvent reposer sur l'utilisation d'informations provenant de parties externes, telles que des plaintes de clients ou des commentaires d'autorités de contrôle, qui peuvent révéler l'existence de problèmes ou faire ressortir des points à améliorer.

Raisons pour lesquelles l'auditeur doit prendre connaissance des sources d'informations utilisées dans le cadre du processus de suivi du système de contrôle interne par l'entité

A120. La connaissance des sources d'informations utilisées dans le cadre du processus de suivi du système de contrôle interne par l'entité, qui porte notamment sur la question de savoir si les informations utilisées sont pertinentes et fiables, aide l'auditeur à évaluer si ce processus est approprié. Lorsque la direction suppose, sans fondement réel, que les informations utilisées pour le suivi sont pertinentes et fiables, des erreurs possibles dans celles-ci pourraient amener la direction à tirer des conclusions incorrectes de ses activités de suivi.

Évaluation du processus de suivi du système de contrôle interne par l'entité (Voir par. 24(c))

Raisons pour lesquelles l'auditeur évalue le caractère approprié du processus de suivi du système de contrôle interne par l'entité

A121. L'évaluation par l'auditeur de la manière dont l'entité procède à des évaluations permanentes et ponctuelles aux fins de suivi de l'efficacité des contrôles l'aide à comprendre si les autres composantes du système de contrôle interne de l'entité ont été mises en œuvre et sont fonctionnelles, et donc à comprendre ces autres composantes. Cette évaluation peut aussi aider l'auditeur à identifier et à évaluer des risques d'anomalies significatives au niveau des états financiers et au niveau des assertions (voir le paragraphe A86).

³⁷ Norme ISA 610 (révisée en 2013), *Utilisation des travaux des auditeurs internes*

Évaluation du caractère approprié du processus de suivi du système de contrôle interne par l'entité (Voir par. 24 (c))

A122. L'auditeur évalue le caractère approprié du processus de suivi du système de contrôle interne par l'entité en fonction de sa connaissance de ce processus.

Système d'information et de communication, et mesures de contrôle (Voir par. 25–26)

A123. Les contrôles des composantes « système d'information et de communication » et « mesures de contrôle » sont principalement des contrôles directs (c'est-à-dire des contrôles qui sont suffisamment précis pour prévenir ou pour détecter et corriger les anomalies au niveau des assertions).

Raisons pour lesquelles l'auditeur doit prendre connaissance du système d'information et de communication ainsi que des contrôles de la composante « mesures de contrôle »

A124. Parce que cela l'aide à identifier et à évaluer les risques d'anomalies significatives au niveau des assertions, l'auditeur est tenu de prendre connaissance du système d'information et de communication de l'entité ce qui implique, d'une part, de comprendre les politiques de l'entité qui définissent le flux des opérations et d'autres aspects des activités de traitement de l'information de l'entité qui sont pertinents pour la préparation des états financiers et, d'autre part, d'évaluer si cette composante contribue adéquatement à la préparation des états financiers de l'entité.. Cette connaissance et cette évaluation peuvent aussi mener à l'identification de risques d'anomalies significatives au niveau des états financiers si, par exemple, les résultats des procédures de l'auditeur ne concordent pas avec les attentes qu'il a définies à l'égard du système de contrôle interne de l'entité en se fondant sur l'information obtenue dans le cadre du processus d'acceptation ou de maintien de la mission (voir le paragraphe A86).

A125. L'auditeur est tenu d'identifier des contrôles spécifiques de la composante « mesures de contrôle », d'évaluer leur conception et de déterminer s'ils ont été mis en œuvre, parce que cela l'aide à comprendre la manière dont la direction répond à certains risques, et parce que cette connaissance lui fournit dès lors une base pour concevoir et mettre en œuvre des procédures d'audit complémentaires adaptées à ces risques, conformément à la norme ISA 330. Plus un risque est considéré comme élevé sur l'échelle de risque inhérent, plus les éléments probants doivent être convaincants. Même si l'auditeur ne prévoit pas de tester l'efficacité du fonctionnement des contrôles identifiés, sa connaissance peut avoir une incidence sur la conception de contrôles de substance dont la nature, le calendrier et l'étendue sont fonction des risques d'anomalies significatives connexes.

Nature itérative de la prise de connaissance et de l'évaluation par l'auditeur du système d'information et de communication ainsi que des mesures de contrôle

A126. Comme il est expliqué au paragraphe A49, la connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable peut aider l'auditeur à définir des attentes initiales concernant les flux d'opérations, les soldes de comptes et les informations à fournir qui peuvent constituer des flux d'opérations importants, des soldes de comptes importants et des informations à fournir importantes. L'auditeur peut s'appuyer sur ces attentes initiales pour délimiter la connaissance qu'il lui faut acquérir des activités de traitement de l'information de l'entité dans le cadre de la prise de connaissance de la composante « système d'information et de communication » qui est exigée au paragraphe 25(a).

A127. La connaissance de l'auditeur relative au système d'information inclut les politiques qui définissent la circulation des informations relatives aux flux d'opérations importants, aux soldes de comptes importants et aux informations à fournir importantes, et les autres aspects connexes des activités de traitement de l'information de l'entité. Ces informations et celles qu'obtient l'auditeur en évaluant le système d'information peuvent confirmer ou avoir une plus grande influence sur les attentes de

l'auditeur concernant les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes initialement identifiés (voir par. A126).

A128. Lorsqu'il acquiert une connaissance de la manière dont l'information relative aux flux d'opérations, aux soldes de comptes et aux informations à fournir importants est intégrée dans le système d'information de l'entité, y circule et en sort, , peut aussi aider l'auditeur à identifier les contrôles de la composante « mesures de contrôle » selon le paragraphe 26 a). Lorsque l'auditeur identifie et évalue les contrôles de la composante « mesures de contrôle », il peut d'abord se concentrer sur les contrôles afférents à certaines écritures comptables et sur les contrôles dont il prévoit de tester l'efficacité du fonctionnement en vue de déterminer la nature, le calendrier et l'étendue des contrôles de substance.

A129. L'évaluation du risque inhérent par l'auditeur peut aussi influencer sur l'identification des contrôles de la composante « mesures de contrôle ». Par exemple, l'identification par l'auditeur des contrôles liés aux risques importants ne peut être réalisées qu'après avoir évalué le risque inhérent au niveau des assertions conformément au paragraphe 31. De plus, les contrôles visant à répondre aux risques pour lesquels l'auditeur a déterminé que des contrôles de substance peuvent ne pas fournir à eux seuls des éléments probants suffisants et appropriés (conformément au paragraphe 33), ne puissent être identifiés que lorsque l'auditeur a complété ses évaluations du risque inhérent.

A130. L'identification et l'évaluation par l'auditeur des risques d'anomalies significatives au niveau des assertions dépendent à la fois :

- de sa connaissance des politiques de l'entité relatives aux activités de traitement de l'information faisant partie de la composante « système d'information et communications » ;
- de son identification et de son évaluation des contrôles de la composante « mesures de contrôle ».

Prise de connaissance du système d'information et de communication (Voir par. 25)

L' Annexe 3 (voir par. 15–19) fournit d'autres exemples d'éléments à prendre en considération concernant le système d'information et de communication .
--

Application proportionnée

A131. Dans les entités peu complexes, le système d'information et les processus opérationnels connexes sont généralement moins sophistiqués que dans les grandes entités et il est probable que l'environnement informatique sera lui aussi moins complexe ; toutefois, cela ne diminue en rien l'importance du rôle du système d'information. Des entités peu complexes dans lesquelles la direction participe directement à l'exploitation peuvent ne pas avoir besoin de descriptions détaillées des procédures comptables, de documents comptables très élaborés, ni de politiques écrites. La prise de connaissance des aspects pertinents du système d'information de l'entité peut donc nécessiter moins d'efforts dans le cadre de l'audit d'entités peu complexes et reposer davantage sur des demandes d'informations que sur l'observation ou l'inspection de documents. Le besoin d'acquérir cette connaissance reste néanmoins important car cette dernière fournit à l'auditeur une base pour concevoir des procédures d'audit complémentaires conformément à la norme ISA 330 et qu'elle peut contribuer à l'identification ou à l'évaluation des risques d'anomalies significatives par l'auditeur (voir par. A86).

Prise de connaissance du système d'information (Voir par. 25(a))

A132. Le système de contrôle interne comprend des aspects qui portent sur les objectifs de l'entité en matière d'information, notamment en matière d'information financière, mais aussi des aspects qui concernent les objectifs d'exploitation ou de conformité, s'ils sont pertinents pour l'information financière. Dans le cadre de la prise de connaissance du système d'information par l'auditeur, la manière dont l'entité initie les opérations et saisit les informations, peut inclure les informations

concernant les systèmes de l'entité (ses politiques) conçus pour l'atteinte d'objectifs d'exploitation et de conformité, étant donné que ces informations sont pertinentes pour la préparation des états financiers. Par ailleurs, lorsqu'une entité dispose d'un système d'information fortement intégré, les contrôles peuvent être conçus de manière à permettre l'atteinte de plusieurs objectifs à la fois, qu'il s'agisse d'objectifs en matière d'information financière, de conformité ou d'exploitation, ou d'une quelconque combinaison de ces objectifs.

A133. La connaissance du système d'information de l'entité comprend également celle des ressources devant servir à mener les activités de traitement de l'information de l'entité. Pour comprendre des risques liés à l'intégrité du système d'information, des informations pertinentes, relatives aux ressources humaines concernées, incluent, :

- la compétence des personnes qui accomplissent les tâches ;
- l'adéquation ou non des ressources aux besoins ;
- l'existence ou non d'une séparation des tâches appropriée.

A134. Pour comprendre les politiques qui définissent la circulation des informations relatives aux flux d'opérations importants, aux soldes de comptes importants et aux informations à fournir importantes dans la composante « système d'information et de communication », l'auditeur peut prendre en considération les éléments suivants :

- (a) les données ou les informations relatives aux opérations et aux autres événements et situations à traiter ;
- (b) le traitement de l'information visant à assurer le maintien de l'intégrité des données ou des informations ;
- (c) les processus, les membres du personnel et les autres ressources qui contribuent au traitement de l'information.

A135. La connaissance des processus opérationnels, qui englobe la manière dont les opérations sont générées, aide l'auditeur à prendre connaissance du système d'information dans le contexte propre à l'entité.

A136. Pour prendre connaissance du système d'information, l'auditeur peut employer différents moyens, dont :

- des demandes d'informations auprès des membres concernés du personnel au sujet des procédures d'initiation, d'enregistrement, de traitement et de communication des opérations ou du processus d'information financière de l'entité ;
- l'inspection des manuels décrivant les politiques ou les processus ou d'autres documents portant sur le système d'information de l'entité ;
- l'observation de l'application des politiques ou des procédures par le personnel de l'entité ;
- la sélection d'opérations et le suivi de leur cheminement dans le processus applicable du système d'information (test de conformité).

Outils et techniques automatisés

A137. L'auditeur peut aussi avoir recours à des techniques automatisées soit pour accéder directement aux bases de données du système d'information de l'entité qui contiennent les documents comptables relatifs aux opérations, soit pour télécharger le contenu de ces bases de données. En appliquant aux informations ainsi obtenues des outils et des techniques automatisés, l'auditeur peut confirmer sa connaissance du flux des opérations dans le système d'information – de leur initiation dans les documents comptables jusqu'à leur enregistrement dans le grand livre – permettant de retracer les écritures comptables ou d'autres enregistrements électroniques, que ce soit pour une opération donnée ou pour l'ensemble des opérations (population entière). L'analyse de vastes ensembles d'opérations, voire d'ensembles complets, peut révéler des écarts par rapport aux

procédures de traitement normales ou prévues, et ainsi permettre l'identification de risques d'anomalies significatives.

Informations ne provenant pas du grand livre et des journaux auxiliaires

A138. Les états financiers peuvent comprendre des informations ne provenant pas du grand livre et des journaux auxiliaires. Des exemples de telles informations que l'auditeur peut prendre en considération peuvent inclure :

- Des informations provenant de contrats de location fournies dans les états financiers pour les informations à fournir dans les états financiers ;
- Des informations fournies dans les états financiers produites par le système de gestion des risques de l'entité ;
- Des informations fournies dans les états financiers en juste valeur et produites par des experts désignés par la direction ;
- Des informations fournies dans les états financiers provenant de modèles ou d'autres calculs ayant servi à établir les estimations comptables comptabilisées ou communiquées dans les états financiers, y compris les informations relatives aux données et hypothèses sous-jacentes utilisées dans ces modèles, par exemple:
 - Les hypothèses élaborées en interne pouvant avoir une incidence sur la durée d'utilisation d'un actif; ou,
 - Les données, comme les taux d'intérêt, qui sont influencées par des facteurs qui échappent à la volonté de l'entité ;
- Des informations fournies dans les états financiers concernant des analyses de sensibilité reposant sur des modèles financiers qui démontrent que la direction a tenu compte d'hypothèses alternatives ;
- Des informations fournies dans les états financiers concernant des analyses de sensibilité reposant sur des modèles financiers qui démontrent que la direction a tenu compte d'hypothèses alternatives ;
- Des informations fournies dans les états financiers provenant d'analyses préparées à l'appui de l'évaluation faite par la direction de la capacité de l'entité à poursuivre son exploitation, comme les informations, s'il en existe, relatives aux événements ou aux situations identifiées susceptibles de jeter un doute important sur cette capacité³⁸.

A139. Certains montants ou informations fournis dans les états financiers de l'entité (comme les informations concernant le risque de crédit, le risque de liquidité et le risque de marché) peuvent être fondés sur des informations provenant du système de gestion des risques de l'entité. Toutefois, l'auditeur n'est pas tenu de comprendre tous les aspects du système de gestion des risques; il exerce son jugement professionnel pour déterminer la connaissance qu'il est nécessaire d'acquérir.

Recours à l'informatique par l'entité dans le contexte du système d'information

Raisons pour lesquelles l'auditeur acquiert une connaissance de l'environnement informatique pertinent au regard du système d'information

A140. La connaissance relative au système d'information qu'acquiert l'auditeur inclut les aspects de l'environnement informatique pertinents au regard du flux des opérations et du traitement de l'information dans le système d'information de l'entité, parce que certains aspects de cet environnement, dont l'utilisation que fait l'entité des applications informatiques, peuvent donner lieu à des risques provenant du recours à l'informatique.

³⁸ Norme ISA 570 (révisée), paragraphes 19–20.

A141. La connaissance du modèle économique de l'entité et de la manière dont le recours à l'informatique y est intégré peut aussi fournir à l'auditeur des éléments de contexte utiles sur la nature et l'étendue du recours à l'informatique qu'il peut s'attendre à voir dans le système d'information.

Connaissance du recours à l'informatique par l'entité

A142. La connaissance qu'acquiert l'auditeur concernant l'environnement informatique peut être axée sur l'identification et la connaissance – du point de vue qualitatif et quantitatif – des applications informatiques particulières et des autres aspects de l'environnement informatique qui sont pertinents au regard du flux des opérations et du traitement de l'information dans le système d'information. Des changements liés au flux des opérations ou au traitement de l'information dans le système d'information peuvent résulter la modification de programmes liés aux applications informatiques ou de la modification directe des données qui se trouvent dans les bases de données servant au traitement ou au stockage des opérations ou des informations.

A143. L'auditeur peut identifier les applications informatiques et l'infrastructure informatique sous-jacente en même temps qu'il acquiert une connaissance de la circulation des informations relatives aux flux d'opérations importants, aux soldes de comptes importants et aux informations à fournir importantes dans le système d'information de l'entité.

Prise de connaissance des communications de l'entité (Voir par. 25(b))

Application proportionnée

A144. Dans les grandes entités plus complexes, les informations que l'auditeur prend en considération pour comprendre les communications de l'entité peuvent être tirées de manuels de procédures et de manuels d'élaboration de l'information financière.

A145. Dans les entités peu complexes, les communications peuvent être moins structurées (par exemple, des manuels formalisés peuvent ne pas être utilisés) en raison du nombre réduit de niveaux hiérarchiques, ainsi que de la plus grande visibilité et disponibilité de la direction. Quelle que soit la taille de l'entité, des voies de communication ouvertes facilitent la communication des exceptions ainsi que leur traitement.

Évaluer si les aspects pertinents du système d'information contribuent à la préparation des états financiers de l'entité (Voir par. 25(c))

A146. Pour évaluer si le système d'information et les communications de l'entité contribuent adéquatement à la préparation des états financiers, l'auditeur se base sur la connaissance qu'il a acquise conformément aux paragraphes 25 (a)–(b).

Mesures de contrôle (Voir par. 26)

Contrôles de la composante « mesures de contrôle »

L'Annexe 3 (paragraphes 20 et 21) fournit d'autres exemples d'éléments à prendre en considération concernant les mesures de contrôle.

A147. La composante « mesures de contrôle » inclut les contrôles – directs et indirects – conçus pour assurer le respect des politiques (qui constituent elles aussi des contrôles) dans toutes les autres composantes du système de contrôle interne.

Exemple :

Les contrôles qu'une entité a mis en œuvre afin de s'assurer que son personnel compte et enregistre correctement les stocks lors de l'inventaire physique annuel sont directement liés aux risques d'anomalies significatives qui ont trait aux assertions sur l'existence et l'exhaustivité du solde du compte de stocks.

A148. L'identification et l'évaluation par l'auditeur de la composante « mesures de contrôle » se concentre sur les contrôles du traitement de l'information, c'est-à-dire les contrôles qui sont appliqués lors du traitement de l'information dans le système d'information de l'entité visant à répondre directement aux risques liés à l'intégrité des informations (c'est-à-dire l'exhaustivité, l'exactitude et la validité des opérations et des autres informations). Toutefois, l'auditeur n'est pas tenu d'identifier et d'évaluer tous les contrôles du traitement de l'information liés aux politiques de l'entité qui définissent, pour les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes, le flux des opérations et d'autres aspects des activités de traitement de l'information de l'entité.

A149. Il se peut aussi que des contrôles directs fassent partie des composantes « environnement de contrôle », « processus d'évaluation des risques par l'entité » ou « processus de suivi du système de contrôle interne par l'entité », lesquels peuvent être identifiés conformément au paragraphe 26. Cependant, plus le lien est indirect entre les contrôles qui favorisent le fonctionnement d'autres contrôles et le contrôle analysé, moins ce contrôle risque d'être efficace pour prévenir, ou détecter et corriger, les anomalies connexes.

Exemple :

L'examen par le directeur des ventes d'une synthèse des ventes pour des magasins spécifiques par région n'est en général lié qu'indirectement aux risques d'anomalies significatives concernant l'assertion relative à l'exhaustivité des ventes. Par conséquent, un tel examen peut être moins efficace pour répondre à ces risques que des contrôles qui y sont plus directement liés, par exemple le rapprochement des documents d'expédition avec les documents de facturation.

A150. Le paragraphe 26 requiert également que l'auditeur identifie et évalue les contrôles généraux informatiques liés aux applications informatiques et aux autres aspects de l'environnement informatique qu'il a jugés comme sujets aux risques provenant du recours à l'informatique, étant donné que les contrôles généraux informatiques favorisent le maintien du fonctionnement efficace des contrôles du traitement de l'information. Un contrôle général informatique ne permet généralement pas à lui seul de répondre à un risque d'anomalies significatives au niveau des assertions.

A151. Les contrôles dont l'auditeur est tenu d'identifier et d'évaluer la conception et la mise en œuvre sont, conformément au paragraphe 26 :

- Des contrôles dont l'auditeur prévoit de tester l'efficacité du fonctionnement en vue de déterminer la nature, le calendrier et l'étendue des contrôles de substance. L'évaluation de ces contrôles fournit à l'auditeur une base pour concevoir des tests de procédures conformément à la norme ISA 330. Parmi ces contrôles, il y a ceux qui visent à répondre aux risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés ;
- des contrôles visant à répondre aux risques importants et les contrôles afférents aux écritures comptables. L'identification et l'évaluation de ces contrôles par l'auditeur peuvent influencer sur sa connaissance des risques d'anomalies significatives et mener à l'identification d'autres risques d'anomalies significatives (voir par. A95). Cette connaissance fournit à l'auditeur une base pour concevoir des contrôles de substance dont la nature, le calendrier et l'étendue sont fonction de l'évaluation des risques d'anomalies significatives connexes ;

- d'autres contrôles qui, selon le jugement professionnel de l'auditeur, sont appropriés pour permettre à celui-ci d'atteindre les objectifs énoncés au paragraphe 13 relatifs aux risques au niveau des assertions.

A152. L'identification des contrôles de la composante « mesures de contrôle » est requise lorsque ceux-ci répondent à au moins un des critères énumérés au paragraphe 26(a). Cependant lorsque plusieurs contrôles permettent chacun d'atteindre le même objectif, il n'est pas nécessaire de tous les identifier.

Types de contrôles de la composante « mesures de contrôle » (Voir par. 26)

A153. Des exemples de contrôles de la composante « mesures de contrôle » incluent notamment les autorisations et les approbations, les rapprochements, les vérifications (comme les contrôles de modification ou de validation ou les calculs automatisés), la séparation de tâches ainsi que les contrôles physiques ou logiques, y compris ceux qui assurent la sauvegarde des actifs.

A154. Des contrôles de la composante « mesures de contrôle » peuvent aussi comprendre des contrôles mis en œuvre par la direction afin de répondre aux risques d'anomalies significatives découlant d'informations n'ayant pas été préparées conformément au référentiel comptable applicable. Ces contrôles peuvent porter sur les informations ne provenant pas du grand livre et des journaux auxiliaires qui sont fournies dans les états financiers.

A155. Qu'ils concernent l'environnement informatique ou les systèmes manuels, les contrôles peuvent avoir divers objectifs et être exécutés à différents niveaux hiérarchiques et fonctionnels.

Application proportionnée (Voir par. 26)

A156. Des contrôles de la composante « mesures de contrôle » pour des entités peu complexes sont généralement semblables à ceux des entités de plus grande taille, mais le formalisme avec lequel ils sont appliqués peut varier. En outre, dans les entités peu complexes, il peut y avoir plus de contrôles effectués directement par la direction.

Exemple :

La seule approbation de la direction pour accorder des délais de paiement aux clients ou pour approuver les achats importants peut fournir un contrôle fort sur les soldes de comptes et les opérations.

A157. Les entités peu complexes ont souvent peu de personnel, ce qui peut limiter dans la pratique la possibilité de séparer les tâches. Cependant, dans une entité détenue par son dirigeant, le propriétaire-dirigeant peut être en mesure d'exercer un contrôle global de l'activité plus efficace que dans une grande entité, ce qui peut compenser les possibilités généralement plus limitées de séparation des tâches. Par contre, comme il est précisé dans la norme ISA 240, la domination de la direction par une seule personne peut constituer une déficience potentielle du contrôle, puisque la direction a alors la possibilité de contourner les contrôles³⁹.

Contrôles visant à répondre aux risques d'anomalies significatives au niveau des assertions (Voir par. 26(a))

Contrôles visant à répondre aux risques identifiés comme des risques importants (Voir par. 26(a)(i))

A158. Qu'il prévoie ou non de tester l'efficacité du fonctionnement des contrôles visant à répondre aux risques importants, l'auditeur peut, pour concevoir et mettre en œuvre des contrôles de substance répondant à ces risques, comme le requiert la norme ISA 330⁴⁰, se baser sur la connaissance acquise relative à la manière dont la direction répond aux risques importants. Bien que les risques

³⁹ Norme ISA 240, paragraphe A28.

⁴⁰ Norme ISA 330, paragraphe 21

associés à des opérations importantes non courantes ou à des questions sujettes à l'exercice d'un jugement soient souvent moins susceptibles de faire l'objet de contrôles non courants, il est possible que la direction ait pris d'autres mesures pour faire face à ces risques. En conséquence, pour comprendre si l'entité a conçu et mis en œuvre des contrôles à l'égard des risques importants associés à de telles opérations et questions, l'auditeur peut notamment se demander si, et comment, la direction répond aux risques. Ces réponses peuvent inclure :

- des contrôles tels qu'un examen des hypothèses par la haute direction ou par des experts ;
- des recours à des processus documentés pour établir des estimations comptables ;
- l'approbation par les personnes constituant le gouvernement d'entreprise.

Exemple :

Dans le cas d'un événement exceptionnel, tel qu'une assignation pour des accusations graves devant un tribunal, l'appréciation de la réponse de l'entité peut inclure le fait de savoir si des experts appropriés (conseillers juridiques internes ou avocats externes par exemple) ont été désignés, si une évaluation de l'incidence potentielle a été faite et de quelle manière la direction entend présenter la situation dans les états financiers.

A159. La norme ISA 240⁴¹ requiert que l'auditeur acquière une connaissance des contrôles liés aux risques d'anomalies significatives résultant de fraudes qu'il a identifiés (ces risques étant considérés comme des risques importants), et explique en outre qu'il est important pour l'auditeur de prendre connaissance des contrôles conçus, mis en œuvre et supervisés par la direction pour prévenir et détecter les fraudes.

Contrôles relatifs aux écritures comptables (Voir par. 26 (a)(ii))

A160. Des contrôles afférents aux écritures comptables visant à répondre aux risques d'anomalies significatives au niveau des assertions, sont censés être identifiés lors de tous les audits, étant donné que le transfert des informations entre les systèmes de traitement des opérations et le grand livre se fait habituellement au moyen d'écritures comptables – courantes ou non, automatisées ou manuelles. Selon la nature de l'entité et la stratégie qu'a définie l'auditeur relatives aux procédures d'audit complémentaires, d'autres contrôles peuvent également être identifiés.

Exemple :

Lorsque l'audit porte sur une entité peu complexe, le système d'information de l'entité peut être simple et l'auditeur ne prévoit pas de s'appuyer sur l'efficacité du fonctionnement des contrôles. En outre, l'auditeur peut n'avoir identifié aucun risque important ou aucun autre risque d'anomalies significatives pour lesquels il est nécessaire d'évaluer la conception des contrôles et à déterminer si ces contrôles ont été mis en œuvre. Lors de cet audit, l'auditeur peut déterminer qu'il n'y a pas d'autres contrôles identifiés que ceux de l'entité sur les écritures comptables.

Outils et techniques automatisés

A161. Dans des systèmes comptables où le grand livre est tenu manuellement, les écritures non standard peuvent être identifiées par la revue de ce grand livre, des journaux auxiliaires ou de la documentation y afférente. Cependant, quand des traitements informatisés sont utilisés pour tenir le grand livre et préparer les états financiers, de telles écritures sont susceptibles d'exister uniquement sous forme électronique et peuvent donc être plus facilement identifiées par l'utilisation des techniques d'audit assistées par ordinateur.

Exemple :

Lorsque l'audit porte sur une entité peu complexe, l'auditeur peut être en mesure d'extraire une liste exhaustive des écritures comptables sous forme de feuille de calcul simple. Grâce à cette feuille de

⁴¹ Norme ISA 240, paragraphes 28 et A33

calcul, l'auditeur peut ainsi trier les écritures comptables en appliquant une variété de filtres tels que la devise ou le nom de la personne ayant effectué la préparation ou la revue, ou les écritures ayant une incidence uniquement sur le bilan ou sur les résultats, etc. ou les trier selon leur date d'enregistrement dans le grand livre, ce qui l'aidera à concevoir des réponses aux risques identifiés relatifs aux écritures comptables.

Contrôles pour lesquels l'auditeur prévoit de tester l'efficacité du fonctionnement (Voir par. 26 (a)(iii))

A162. L'auditeur détermine s'il existe des risques d'anomalies significatives au niveau des assertions pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés. La norme ISA 330⁴² requiert que l'auditeur conçoive et mette en œuvre des tests de procédures visant à répondre à ces risques lorsque des contrôles de substance seuls ne peuvent fournir des éléments probants suffisants et appropriés au niveau des assertions. Ces contrôles, lorsqu'il en existe, doivent alors être identifiés et évalués.

A163. Dans les autres cas, si l'auditeur prévoit de tenir compte de l'efficacité du fonctionnement des contrôles pour déterminer, conformément à la norme ISA 330, la nature, le calendrier et l'étendue des contrôles de substance, ces contrôles doivent aussi être identifiés, puisque la norme ISA 330⁴³ requiert que l'auditeur conçoive et mette en œuvre des tests à leur égard.

Exemple :

L'auditeur peut prévoir de tester l'efficacité du fonctionnement :

- des contrôles afférents aux flux d'opérations courantes, car il s'agit parfois de l'approche la plus efficace ou la plus efficiente lorsqu'il y a un grand nombre d'opérations homogènes ;
- des contrôles liés à l'exhaustivité et à l'exactitude des informations produites par l'entité (par exemple des contrôles afférents à la préparation des rapports générés par le système), pour s'assurer de la fiabilité de ces informations, s'il prévoit de tenir compte de l'efficacité du fonctionnement de ces contrôles dans la conception et la mise en œuvre des procédures d'audit complémentaires ;
- des contrôles liés aux objectifs d'exploitation et de conformité s'ils ont trait à des données que l'auditeur évalue ou utilise dans le cadre de ses procédures d'audit.

A164. Les risques d'anomalies significatives identifiés par l'auditeur au niveau des états financiers peuvent aussi avoir une incidence sur sa planification visant à tester l'efficacité du fonctionnement des contrôles. Par exemple, si l'auditeur relève des déficiences dans l'environnement de contrôle, cela peut influencer sur ses attentes quant à l'efficacité du fonctionnement des contrôles directs en général.

Autres contrôles que l'auditeur juge appropriés (Voir par. 26(a)(iv))

A165. Des exemples d'autres contrôles que l'auditeur, selon son jugement, peut juger utile d'identifier, d'évaluer la conception et d'en vérifier la mise en œuvre comprennent :

- les contrôles visant à répondre aux risques dont l'évaluation se situe dans la partie supérieure de l'échelle de risque inhérent, mais qui ne sont pas identifiés comme des risques importants ;
- les contrôles liés au rapprochement entre les documents comptables détaillés et le grand livre ;
- les contrôles complémentaires de l'entité utilisatrice, si l'entité fait appel à une société de services⁴⁴.

⁴² Norme ISA 330, par. 8 (b)

⁴³ Norme ISA 330, par. 8 (a)

⁴⁴ Norme ISA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*

Identification des applications informatiques et des autres aspects de l'environnement informatique, identification des risques provenant du recours à l'informatique, et identification des contrôles généraux informatiques (Voir par. 26(b)–(c))

L'**Annexe 5** présente des exemples concernant des caractéristiques pouvant être pertinentes pour l'identification des applications informatiques et des autres aspects de l'environnement informatique qui sont sujets aux risques provenant du recours à l'informatique, .

Identification des applications informatiques et des autres aspects de l'environnement informatique (Voir par. 26(b))

Raisons pour lesquelles l'auditeur identifie les risques provenant du recours à l'informatique ainsi que les contrôles généraux informatiques liés aux applications informatiques et aux autres aspects de l'environnement informatique qu'il a identifiés

A166. La connaissance des risques provenant du recours à l'informatique et des contrôles généraux informatiques mis en œuvre par l'entité pour y répondre peut avoir une incidence sur :

- la décision de l'auditeur de tester ou non l'efficacité du fonctionnement des contrôles visant à répondre aux risques d'anomalies significatives au niveau des assertions ;

Exemple :

Lorsqu'en raison d'une conception inefficace ou d'une mise en œuvre inadéquate, les contrôles généraux informatiques ne permettent pas de répondre aux risques découlant du recours à l'informatique (par exemple parce qu'ils ne permettent pas de prévenir ou de détecter adéquatement la modification non autorisée des programmes ou l'accès non autorisé aux applications informatiques), cette situation peut influencer sur la décision de l'auditeur de s'appuyer ou non sur les contrôles automatisés qui font partie des applications informatiques impactées.

- l'évaluation par l'auditeur du risque lié au contrôle interne au niveau des assertions ;

Exemple :

Le maintien de l'efficacité du fonctionnement d'un contrôle du traitement de l'information peut dépendre de certains contrôles généraux informatiques qui préviennent ou détectent la modification non autorisée des programmes liés au contrôle du traitement de l'information (c'est-à-dire des contrôles qui préviennent ou détectent la modification de programmes liés aux applications informatiques associées). L'efficacité (ou l'inefficacité) attendue du fonctionnement des contrôles généraux informatiques peut alors influencer sur l'évaluation par l'auditeur du risque lié au contrôle interne. Ainsi, le risque lié au contrôle interne est susceptible d'être plus élevé si l'auditeur s'attend à ce que les contrôles généraux informatiques concernés soient inefficaces ou s'il ne prévoit pas de tester ces contrôles.

- la stratégie de l'auditeur afin de tester les informations de l'entité générées par les applications informatiques de celle-ci ou produites au moyen d'informations tirées de ces applications ;

Exemple :

Lorsque des informations produites par l'entité devant servir d'éléments probants ont été générées par des applications informatiques, l'auditeur peut décider de tester les contrôles afférents aux rapports générés par le système incluant l'identification et le test des contrôles généraux informatiques qui visent à répondre aux risques de modification non autorisée ou inappropriée (qu'il s'agisse de modification des programmes ou de modification directe des données des rapports).

- l'évaluation par l'auditeur du risque inhérent au niveau des assertions ;ou

Exemple :

Des modifications importantes apportées à la programmation d'une application informatique pour tenir compte d'exigences nouvelles ou révisées du référentiel comptable applicable peuvent être un indicateur de la complexité de ces nouvelles exigences et de leur incidence sur les états financiers de l'entité. De plus, lorsque de telles modifications importantes sont apportées à la programmation ou aux données d'une application informatique, celle-ci est susceptible d'être sujette aux risques provenant du recours à l'informatique.

- la conception de procédures d'audit complémentaires.

Exemple :

Lorsque les contrôles du traitement de l'information dépendent des contrôles généraux informatiques, l'auditeur peut décider de tester l'efficacité du fonctionnement des contrôles généraux informatiques, ce qui requerra la conception de tests de procédures pour ceux-ci. Si, dans les mêmes circonstances, l'auditeur décide de ne pas tester l'efficacité du fonctionnement des contrôles généraux informatiques, ou qu'il s'attend à ce que ces contrôles soient inefficaces, il peut être nécessaire de répondre aux risques associés provenant du recours à l'informatique en concevant des contrôles de substance. Cependant, si ces risques associés sont liés à des risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés, il se peut qu'il ne soit pas possible d'y répondre. L'auditeur pourrait alors devoir considérer l'incidence de cette situation sur son opinion d'audit.

Identification des applications informatiques qui sont sujettes aux risques provenant du recours à l'informatique

A167. Concernant les applications informatiques pertinentes au regard du système d'information, la connaissance de la nature et de la complexité des processus informatiques particuliers et des contrôles généraux informatiques que l'entité a mis en œuvre peuvent aider l'auditeur à identifier les applications informatiques sur lesquelles l'entité s'appuie pour assurer l'exactitude du traitement et le maintien de l'intégrité des informations dans son système d'information. Ces applications informatiques peuvent être sujettes aux risques provenant du recours à l'informatique.

A168. L'identification des applications informatiques sujettes aux risques provenant du recours à l'informatique implique la prise en considération des contrôles identifiés par l'auditeur, puisque ces contrôles peuvent impliquer l'utilisation de l'informatique, ou s'appuyer sur celle-ci. L'auditeur peut se concentrer sur la question de savoir si une application informatique comporte des contrôles automatisés qu'il a identifiés et sur lesquels la direction s'appuie, notamment des contrôles visant à répondre aux risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés. L'auditeur peut aussi considérer la manière dont les informations relatives aux flux d'opérations importants, aux soldes de comptes importants et aux informations à fournir importantes sont stockées et traitées dans le système d'information, et si la direction s'appuie sur les contrôles généraux informatiques pour assurer le maintien de l'intégrité de ces informations.

A169. Les contrôles identifiés par l'auditeur peuvent dépendre de rapports générés par le système, auquel cas les applications informatiques produisant ces rapports peuvent être jugées sujettes aux risques provenant du recours à l'informatique. Dans d'autres cas, l'auditeur peut ne pas prévoir de s'appuyer sur les contrôles afférents aux rapports générés par le système mais plutôt de tester directement les données d'entrée et de sortie de ces rapports et ainsi, il se peut qu'il n'identifie pas les applications informatiques associées comme étant sujettes aux risques provenant du recours à l'informatique.

Application proportionnée

A170. L'étendue de la connaissance qu'acquiert l'auditeur concernant les processus informatiques – notamment en ce qui concerne la mesure dans laquelle l'entité a mis en œuvre des contrôles

généraux informatiques – variera selon la nature et les circonstances de l'entité, son environnement informatique, ainsi que la nature et l'étendue des contrôles identifiés par l'auditeur. Le nombre d'applications informatiques sujettes aux risques provenant du recours à l'informatique variera aussi en fonction de ces facteurs.

Exemples :

- Une entité qui utilise un logiciel disponible sur le marché et qui, faute de pouvoir accéder au code source, ne peut apporter aucune modification au programme n'aura probablement pas de processus établi pour ce type de modification. Il pourrait toutefois y avoir un processus ou des procédures pour la configuration du logiciel (plan de comptes, paramètres de l'information, seuils, etc.) et la gestion des accès à l'application (octroi d'un accès administrateur au logiciel disponible sur le marché, par exemple). Dans de telles circonstances, il est peu probable que l'entité ait mis en œuvre ou ait besoin de contrôles généraux informatiques formalisés.
- En revanche, dans une plus grande entité, le recours à l'informatique peut être plus important et l'environnement informatique peut comporter de nombreuses applications informatiques, gérées au moyen de processus informatiques complexes (par exemple, l'existence d'un service informatique spécifique qui s'occupe du développement et de la mise en œuvre des modifications apportées aux programmes ainsi que de la gestion des droits d'accès), incluant des contrôles généraux informatiques formalisés au travers de ses processus informatiques.
- Lorsque la direction ne s'appuie pas sur des contrôles automatisés ni sur des contrôles généraux informatiques pour le traitement des opérations et le maintien de l'intégrité des données, et qu'aucun contrôle automatisé ni autre contrôle du traitement de l'information (ou contrôle qui dépend des contrôles généraux informatiques) n'est identifié par l'auditeur, celui-ci peut prévoir de tester directement les informations produites par l'entité qui ont nécessité un recours à l'informatique, et de n'identifier aucune application informatique sujette aux risques provenant du recours à l'informatique.
- Lorsque la direction s'appuie sur une application informatique pour le traitement ou le maintien de l'intégrité des données, que le volume de données est important, et qu'elle s'appuie sur l'application informatique pour l'exécution de contrôles automatisés que l'auditeur a identifiés, il est probable que l'application informatique soit sujette aux risques provenant du recours à l'informatique.

A171. Lorsque l'environnement informatique d'une l'entité est particulièrement complexe, il est probable de requérir l'implication dans l'équipe de membres possédant des compétences spécialisées en informatique qui seront appelés à l'identification des applications informatiques et des autres aspects de l'environnement informatique, des risques associés provenant du recours à l'informatique et des contrôles généraux informatiques. La contribution de ces membres dans un environnement informatique complexe sera probablement essentielle et étendue.

Identification des autres aspects de l'environnement informatique qui sont sujets aux risques provenant du recours à l'informatique

A172. Les autres aspects de l'environnement informatique qui peuvent être sujets aux risques provenant du recours à l'informatique comprennent le réseau, le système d'exploitation et les bases de données, ainsi que – dans certaines circonstances – les interfaces entre les applications informatiques. Lorsque l'auditeur n'identifie pas d'applications informatiques sujettes aux risques provenant du recours à l'informatique, d'autres aspects de l'environnement informatique ne sont généralement pas identifiés. Lorsque l'auditeur a identifié des applications informatiques sujettes aux risques provenant du recours à l'informatique, d'autres aspects de l'environnement informatique (par exemple les bases de données, le système d'exploitation ou le réseau) sont probablement identifiés parce que ceux-ci soutiennent les applications informatiques identifiées et interagissent avec elles.

Identification des risques provenant du recours à l'informatique et identification des contrôles généraux informatiques (Voir par. 26(c))

L'Annexe 6 présente des exemples d'éléments à prendre en considération pour prendre connaissance des contrôles généraux informatiques.

A173. Lors de l'identification des risques provenant du recours à l'informatique, l'auditeur peut prendre en considération la nature des applications informatiques ou des autres aspects de l'environnement informatique qu'il a identifiés ainsi que les raisons pour lesquelles ces applications ou ces autres aspects sont sujettes aux risques provenant du recours à l'informatique. Pour certaines applications informatiques ou certains autres aspects de l'environnement informatique, l'auditeur peut identifier des risques associés provenant du recours à l'informatique qui concernent surtout l'accès – ou les modifications – non autorisé aux programmes, ou la modification inappropriée des données (par exemple, des risques de modification inappropriée des données résultant d'un accès direct aux bases de données ou de la possibilité de manipuler directement les informations).

A174. L'étendue et la nature des risques associés provenant du recours à l'informatique varient selon la nature et les caractéristiques des applications informatiques et des autres aspects de l'environnement informatique qui sont identifiés. Certains risques associés liés à l'informatique peuvent être attribuables au fait que l'entité confie certains aspects identifiés de son environnement informatique à des fournisseurs de services internes ou externes (par exemple, en ayant recours aux services d'hébergement de tiers pour son environnement informatique ou en confiant la gestion de ses processus informatiques au centre de services partagés du groupe auquel elle appartient). Il se peut aussi que l'auditeur identifie des risques associés provenant du recours à l'informatique qui sont liés à la cybersécurité. Il est plus que probable que les risques provenant du recours à l'informatique soient d'autant plus nombreux que les contrôles des applications qui sont automatisés sont nombreux ou complexes et que la direction s'appuie fortement sur ces contrôles pour assurer le traitement efficace des opérations ou le maintien efficace de l'intégrité des informations sous-jacentes.

Évaluation de la conception des contrôles identifiés de la composante « mesures de contrôle », et vérification de leur mise en œuvre (Voir par. 26(d))

A175. L'évaluation de la conception d'un contrôle implique de l'auditeur de déterminer si le contrôle, seul ou combiné avec d'autres contrôles, est capable de prévenir, ou de détecter et de corriger effectivement, les anomalies significatives (c'est-à-dire l'objectif de contrôle).

A176. Pour déterminer si un contrôle identifié a été mis en œuvre, l'auditeur s'assure que ce contrôle existe et que l'entité l'applique. Il y a peu d'intérêt à évaluer la mise en œuvre d'un contrôle qui n'est concrètement pas conçu. C'est pourquoi, l'auditeur évalue d'abord la conception d'un contrôle. Un contrôle mal conçu peut constituer une déficience du contrôle.

A177. Les procédures d'évaluation des risques pour recueillir des éléments probants relatifs à la conception et à la mise en œuvre des contrôles pertinents de la composante « mesures de contrôle » peuvent comprendre :

- des demandes d'informations auprès du personnel de l'entité ;
- la vérification de l'application de contrôles spécifiques ;
- la prise de connaissance de documents et de rapports.

Les demandes d'informations seules ne sont cependant pas suffisantes pour atteindre les objectifs de ces procédures.

A178. L'auditeur peut s'attendre, sur la base de l'expérience acquise lors de l'audit précédent ou des procédures d'évaluation des risques mises en œuvre pour la période en cours, à ce que les contrôles visant à répondre à un risque important n'aient pas été conçus efficacement ou qu'ils n'aient pas été mis en œuvre par la direction. Dans de telles circonstances, les procédures mises en œuvre pour remplir l'exigence énoncée au paragraphe 26 d) peuvent consister à vérifier que les contrôles n'ont

pas été conçus efficacement ou qu'ils n'ont pas été mis en œuvre. Si les résultats des procédures indiquent que des contrôles ont été nouvellement conçus ou mis en œuvre, l'auditeur met en œuvre les procédures mentionnées aux paragraphes 26(b)–(d) à l'égard de ces contrôles.

A179. Lorsqu'un contrôle a été conçu efficacement et mis en œuvre, l'auditeur peut conclure qu'il serait approprié de le tester afin de tenir compte de l'efficacité de son fonctionnement dans la conception des contrôles de substance. Toutefois, il n'y a aucune utilité à tester un contrôle dont la conception ou la mise en œuvre est inefficace. Lorsque l'auditeur prévoit de tester un contrôle, l'information obtenue sur la mesure dans laquelle ce contrôle permet de répondre à un ou à plusieurs risques d'anomalies significatives est prise en considération lors de l'évaluation du risque lié au contrôle interne au niveau des assertions.

A180. Pour tester l'efficacité du fonctionnement des contrôles identifiés de la composante « mesures de contrôle », il ne suffit pas d'évaluer leur conception et de vérifier leur mise en œuvre. En ce qui a trait aux contrôles automatisés, l'auditeur peut cependant prévoir de tester l'efficacité du fonctionnement des contrôles identifiés non pas en testant ces derniers directement, mais plutôt en identifiant et en testant les contrôles généraux informatiques qui en assurent le fonctionnement systématique. L'obtention d'éléments probants attestant la mise en œuvre d'un contrôle manuel à un moment précis ne fournit pas d'éléments probants quant à son fonctionnement efficace à d'autres moments au cours de la période auditée. Les tests de l'efficacité du fonctionnement des contrôles, y compris des contrôles indirects, sont décrits plus en détail dans la norme ISA 330⁴⁵.

A181. Lorsque l'auditeur ne prévoit pas de tester l'efficacité du fonctionnement de contrôles identifiés, sa connaissance peut l'aider à concevoir des contrôles de substance dont la nature, le calendrier et l'étendue sont fonction des risques d'anomalies significatives connexes.

Exemple :

Les résultats des procédures d'évaluation des risques peuvent fournir à l'auditeur une base pour la prise en compte, lors de la conception des sondages, des écarts pouvant affecter une population.

Déficiences de contrôle dans le système de contrôle interne de l'entité (Voir par. 27)

A182. Lors de l'évaluation de chacune des composantes du système de contrôle interne de l'entité⁴⁶, l'auditeur peut déterminer que certaines des politiques de l'entité se rapportant à une composante donnée ne sont pas appropriées à la nature et aux circonstances de l'entité. Cela peut donner à l'auditeur des indices qui l'assisteront à relever des déficiences de contrôle. Si l'auditeur a relevé une ou plusieurs déficiences de contrôle, il peut prendre en considération l'incidence de ces déficiences sur les procédures d'audit complémentaires à concevoir conformément à la norme ISA 330.

A183. Si l'auditeur a relevé une ou plusieurs déficiences de contrôle, la norme ISA 265⁴⁷ requiert qu'il détermine si, individuellement ou en association, elles constituent des déficiences importantes. L'auditeur exerce son jugement professionnel pour déterminer si une déficience de contrôle constitue une déficience importante⁴⁸.

⁴⁵ Norme ISA 330, paragraphes 8–11

⁴⁶ Paragraphes 21(b), 22(b), 24(c), 25(c) et 26(d)

⁴⁷ Norme ISA 265, *Communication des déficiences dans le contrôle interne aux responsables de la gouvernance et à la direction*, paragraphe 8.

⁴⁸ Les paragraphes A6–A7 de la norme ISA 265 énoncent des indices de déficiences importantes ainsi que des points à prendre en considération pour déterminer si une déficience ou une combinaison de déficiences constitue une déficience importante.

Exemples :

Exemples de situations pouvant indiquer l'existence d'une déficience importante du contrôle :

- la détection d'une fraude de quelque ampleur que ce soit impliquant la haute direction ;
- l'identification de processus internes inadéquats liés à la communication de déficiences relevées par la fonction d'audit interne ;
- la présence de déficiences déjà communiquées et n'ayant pas été corrigées en temps opportun par la direction ;
- le fait que la direction n'ait pas répondu à des risques importants (par exemple, aucun contrôle mis en œuvre relatif à ces risques) ;
- le retraitement d'états financiers déjà publiés.

Identification et évaluation des risques d'anomalies significatives (Voir par. 28–37)

Raisons pour lesquelles l'auditeur identifie et évalue les risques d'anomalies significatives

A184. L'auditeur identifie et évalue les risques d'anomalies significatives pour déterminer la nature, le calendrier et l'étendue des procédures d'audit complémentaires nécessaires à l'obtention d'éléments probants suffisants et appropriés. Grâce à ces éléments probants, l'auditeur est en mesure d'exprimer sur les états financiers une opinion présentant un risque d'audit suffisamment faible.

A185. Les informations rassemblées lors de la mise en œuvre des procédures d'évaluation des risques sont utilisées comme éléments probants à l'appui de l'identification et de l'évaluation des risques d'anomalies significatives. Par exemple, les éléments probants que l'auditeur obtient en évaluant la conception des contrôles identifiés et en déterminant si ces contrôles ont été mis en œuvre dans la composante « mesures de contrôle » sont utilisés à l'appui de son évaluation des risques. Ces éléments probants fournissent aussi à l'auditeur une base pour concevoir une approche générale adaptée à son évaluation des risques d'anomalies significatives au niveau des états financiers, et pour concevoir et mettre en œuvre des procédures d'audit complémentaires dont la nature, le calendrier et l'étendue sont fonction de son évaluation des risques d'anomalies significatives au niveau des assertions, conformément à la norme ISA 330.

Identification des risques d'anomalies significatives (Voir par. 28)

A186. L'auditeur identifie les risques d'anomalies significatives avant prise en considération des contrôles y afférents (c'est-à-dire le risque inhérent), en se fondant sur son analyse préliminaire des anomalies qui ont une possibilité raisonnable de se concrétiser et d'être significatives si elles se concrétisent⁴⁹.

A187. Comme elle fournit aussi une base pour la détermination des assertions pertinentes, l'identification des risques d'anomalies significatives assiste l'auditeur à identifier les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes.

Assertions

Raisons pour lesquelles l'auditeur se réfère aux assertions

A188. Lorsqu'il identifie et évalue les risques d'anomalies significatives, l'auditeur se réfère aux assertions pour examiner les différents types d'anomalies susceptibles de se produire. Les assertions pour lesquelles un risque d'anomalies significatives a été identifié par l'auditeur constituent des assertions pertinentes.

⁴⁹ Norme ISA 200, paragraphe A15(a).

Utilisation des assertions

A189. Lorsqu'il identifie et évalue les risques d'anomalies significatives, l'auditeur peut utiliser les catégories d'assertions mentionnées aux paragraphes A190 (a)–(b) ci-après, ou encore les exprimer différemment pourvu que tous les aspects ci-dessous soient couverts. Il peut choisir de combiner les assertions concernant les flux d'opérations et les événements, ainsi que les informations à fournir les concernant, avec celles concernant les soldes de comptes et les informations à fournir les concernant.

A190. Les assertions auxquelles l'auditeur se réfère lorsqu'il prend en considération les différents types d'anomalies potentielles peuvent correspondre aux catégories suivantes :

- (a) les assertions concernant les flux d'opérations et les événements de la période auditée, ainsi que les informations à fournir les concernant :
 - (i) réalité : Les opérations ou les événements qui ont été comptabilisés, ou pour lesquels des informations ont été fournies, se sont produits et se rapportent à l'entité,
 - (ii) exhaustivité : Toutes les opérations et tous les événements qui devaient être comptabilisés ont été enregistrés, et toutes les informations à fournir les concernant qui auraient dû être présentées dans les états financiers l'ont bien été,
 - (iii) exactitude : Les montants et autres données relatives à des opérations ou événements comptabilisés l'ont été correctement, et les informations à fournir les concernant ont été évaluées et présentées de manière appropriée,
 - (iv) séparation des périodes : Les opérations et événements ont été comptabilisés dans la bonne période comptable,
 - (v) classification : Les opérations et les événements ont été enregistrés dans les bons comptes,
 - (vi) présentation : Les opérations et les événements sont regroupés ou ventilés de manière appropriée et sont décrits clairement, et les informations à fournir les concernant sont pertinentes et compréhensibles, compte tenu des exigences du référentiel comptable applicable ;

- (b) les assertions concernant les soldes de comptes en fin de période, ainsi que les informations à fournir les concernant :
 - (i) existence : Les actifs, les passifs et les fonds propres existent,
 - (ii) droits et obligations : L'entité détient un droit sur les actifs ou le contrôle, et les passifs reflètent les obligations de l'entité,
 - (iii) exhaustivité : Tous les actifs, les passifs et les fonds propres qui devraient être comptabilisés ont été enregistrés, et toutes les informations à fournir les concernant qui auraient dû être présentées dans les états financiers l'ont bien été,
 - (iv) exactitude, évaluation et imputation : Les actifs, les passifs et les fonds propres ont été présentés dans les états financiers pour leur bonne valeur et tous les ajustements résultant de leur valorisation ou de leur dépréciation ont été enregistrés de façon appropriée, et les informations à fournir les concernant ont été évaluées et présentées de manière appropriée,
 - (v) classification : Les actifs, les passifs et les éléments de capitaux propres ont été enregistrés dans les bons comptes,
 - (vi) présentation : Les actifs, les passifs et les éléments de capitaux propres sont regroupés ou ventilés de manière appropriée et sont décrits clairement, et les informations à fournir les concernant sont pertinentes et intelligibles, compte tenu des exigences du référentiel comptable applicable.

A191. L'auditeur peut également se référer aux assertions mentionnées aux paragraphes A190 (a)–(b), en les adaptant au besoin, lorsqu'il prend en considération les différents types d'anomalies pouvant

survenir dans les informations fournies qui ne sont pas directement liées à des flux d'opérations, événements ou soldes de comptes enregistrés.

Exemple :

L'entité peut être tenue, selon le référentiel comptable applicable, de décrire son exposition aux risques découlant d'instruments financiers et de préciser l'origine des risques, les objectifs, politiques et processus relatifs à la gestion des risques, et les méthodes suivies pour évaluer ces risques.

Considérations propres aux entités du secteur public

A192. Dans le cadre de ses assertions sur les états financiers, complémentairement aux assertions mentionnées aux paragraphes A190 (a)–(b), la direction d'une entité du secteur public peut souvent déclarer que les opérations et événements ont été réalisés conformément à la législation, la réglementation ou les instructions d'une autre autorité. De telles assertions peuvent être incluses dans l'étendue de l'audit des états financiers.

Risques d'anomalies significatives au niveau des états financiers (Voir par. 28(a) et 30)

Raisons pour lesquelles l'auditeur identifie et évalue les risques d'anomalies significatives au niveau des états financiers

A193. L'auditeur identifie les risques d'anomalies significatives au niveau des états financiers pour déterminer si ces risques ont un effet diffus sur les états financiers et si, de ce fait, ils nécessitent une approche générale selon la norme ISA 330⁵⁰.

A194. Les risques d'anomalies significatives au niveau des états financiers peuvent aussi avoir une incidence sur les assertions individuelles, et l'identification de ces risques peut assister l'auditeur à évaluer les risques d'anomalies significatives au niveau des assertions ainsi qu'à concevoir des procédures d'audit complémentaires pour répondre aux risques identifiés.

Identification et évaluation des risques d'anomalies significatives au niveau des états financiers

A195. Les risques d'anomalies significatives au niveau des états financiers se réfèrent aux risques qui affectent de façon diffuse les états financiers pris dans leur ensemble et qui peuvent potentiellement affecter plusieurs assertions. Les risques de cette nature ne sont pas nécessairement identifiables au niveau des flux d'opérations, des soldes de compte ou des informations fournies dans les états financiers (par exemple à cause du contournement du contrôle interne par la direction). Ils sont plutôt le résultat de circonstances qui augmentent les risques d'anomalies significatives au niveau des assertions. Le fait d'évaluer si les risques identifiés affectent de manière diffuse les états financiers permet à l'auditeur de fonder son évaluation des risques d'anomalies significatives au niveau des états financiers. Dans d'autres cas, l'auditeur peut également identifier plusieurs assertions qui sont susceptibles d'être affectées par le risque, ce qui peut avoir des conséquences sur l'identification et l'évaluation des risques d'anomalies significatives au niveau des assertions.

Exemple :

Confrontée à des pertes d'exploitation et des problèmes de trésorerie, l'entité compte sur un financement – qu'elle n'a pas encore obtenu – pour poursuivre ses activités. L'auditeur peut alors déterminer que l'application du principe comptable de continuité d'exploitation donne lieu à un risque d'anomalies significatives au niveau des états financiers. Dans cette situation, il pourrait être nécessaire d'appliquer un référentiel comptable sur la base de valeurs liquidatives, ce qui aurait probablement un effet diffus sur l'ensemble des assertions.

A196. L'identification et l'évaluation par l'auditeur des risques d'anomalies significatives au niveau des états financiers dépendent de sa connaissance du système de contrôle interne de l'entité (en particulier

⁵⁰ Norme ISA 330, paragraphe 5

de l'environnement de contrôle, du processus d'évaluation des risques par l'entité et du processus de suivi du système de contrôle interne par l'entité) ainsi que :

- du résultat des évaluations connexes requises par les paragraphes 21(b), 22(b), 24(c) et 25(c) ;
- de toute déficience du contrôle relevée en application du paragraphe 27.

Plus particulièrement, les risques au niveau des états financiers peuvent provenir de déficiences dans l'environnement de contrôle ou d'événements ou de situations externes, comme une détérioration de la conjoncture économique.

A197. La prise en compte des risques d'anomalies significatives résultant de fraudes peut être particulièrement pertinente lorsque l'auditeur analyse les risques d'anomalies significatives au niveau des états financiers.

Exemple :

Lors de demandes d'informations auprès de la direction, l'auditeur comprend que les états financiers de l'entité seront utilisés dans le cadre de discussions avec des prêteurs pour l'obtention de financement supplémentaire visant à maintenir un fonds de roulement. Il peut ainsi déterminer qu'une plus grande possibilité d'anomalies est présente en raison de facteurs de risque de fraude qui influent sur le risque inhérent (à savoir la possibilité que les états financiers comportent des anomalies significatives résultant de facteurs de risque ayant rapport aux informations financières mensongères, comme la surévaluation des actifs et des produits ainsi que la sous-évaluation des passifs et des charges pour favoriser l'obtention du financement).

A198. La connaissance de l'environnement de contrôle et des autres composantes du système de contrôle interne acquise par l'auditeur, notamment dans le cadre des évaluations connexes, peut amener celui-ci à douter de sa capacité à recueillir des éléments probants sur lesquels fonder son opinion d'audit, voire l'amener à se démettre de la mission lorsqu'il est possible de le faire selon la législation ou la réglementation applicable.

Exemples :

- Après avoir évalué l'environnement de contrôle de l'entité, l'auditeur a des préoccupations au sujet de l'intégrité de la direction de l'entité qui peuvent être assez graves pour l'amener à conclure que le risque que la direction ait intentionnellement inclus de fausses déclarations dans les états financiers est tel qu'il lui est impossible de réaliser l'audit.
- Après avoir évalué le système d'information et les communications de l'entité, l'auditeur détermine l'existence d'une mauvaise gestion des changements importants apportés à l'environnement informatique, la surveillance exercée par la direction et les personnes constituant le gouvernement d'entreprise ayant été minime. L'état et la fiabilité des documents comptables de l'entité soulèvent donc des préoccupations importantes pour l'auditeur. Dans de tels situations, celui-ci peut conclure qu'il ne sera probablement pas en mesure de recueillir des éléments probants suffisants et appropriés pour fonder une opinion non modifiée sur les états financiers.

A199. La norme ISA 705 (révisée)⁵¹ définit des diligences et fournit des modalités d'application sur la détermination des cas où l'auditeur se trouve amené à exprimer une opinion avec réserve ou à formuler une impossibilité d'exprimer une opinion ou, comme il peut être nécessaire dans certains cas, à se démettre de la mission lorsqu'il est possible de le faire selon la législation ou la réglementation applicable.

⁵¹ Norme ISA 705 (révisée), *Expression d'une opinion modifiée dans le rapport de l'auditeur indépendant*.

Considérations propres aux entités du secteur public

A200. Dans le cas des entités du secteur public, l'identification des risques au niveau des états financiers peut se faire en tenant compte, entre autres, de questions relatives au climat politique, à l'intérêt public ou au caractère délicat des programmes concernés.

Risques d'anomalies significatives au niveau des assertions (Voir par. 28(b))

L'Annexe 2 fournit des exemples, dans le contexte des facteurs de risque inhérent, d'événements et de situations pouvant indiquer l'existence possible d'anomalies qui peuvent s'avérer significatives .

A201. Les risques d'anomalies significatives qui ne touchent pas les états financiers de manière diffuse sont des risques d'anomalies significatives au niveau des assertions.

Assertions pertinentes, et flux d'opérations importants, soldes de comptes importants et informations à fournir importantes (Voir par. 29)

Raisons pour lesquelles l'auditeur détermine les assertions pertinentes ainsi que les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes

A202. La détermination des assertions pertinentes ainsi que des flux d'opérations importants, des soldes de comptes importants et des informations à fournir importantes fournit à l'auditeur une base pour délimiter la connaissance qu'il doit acquérir du système d'information de l'entité conformément au paragraphe 25(a). Cette connaissance peut de plus assister l'auditeur à identifier et à évaluer les risques d'anomalies significatives (voir par. A86).

Outils et techniques automatisés

A203. L'auditeur peut avoir recours à des techniques automatisées pour faciliter l'identification des flux d'opérations importants, des soldes de comptes importants et des informations à fournir importantes.

Exemples :

- Pour comprendre la nature, la source, la taille et le volume des opérations d'une population donnée, il est possible d'analyser celle-ci dans son ensemble au moyen d'outils et de techniques automatisés. L'application de techniques automatisées peut notamment permettre à l'auditeur de voir qu'un compte à solde nul en fin de période se compose de nombreuses opérations et écritures comptables effectuées durant la période et qui se compensent, ce qui indique que le solde de compte ou le flux d'opérations peut être important (ce peut être le cas d'un compte provisoire pour la paie, par exemple). Par ailleurs, l'analyse d'un compte provisoire pour la paie peut faire ressortir des frais remboursés à la direction (et à d'autres employés). Comme ces remboursements sont versés à des parties liées, il pourrait s'agir d'une information à fournir importante.
- Grâce à l'analyse des flux de la totalité des opérations génératrices de produits, l'auditeur peut plus facilement identifier un flux d'opérations important qui n'avait pas été identifié précédemment.

Informations à fournir qui peuvent être importantes

A204. Les informations à fournir importantes comprennent les informations tant quantitatives que qualitatives auxquelles sont associées une ou plusieurs assertions pertinentes. Des exemples d'informations à fournir qui ont des aspects qualitatifs et qui, en raison de leur éventuelle association à des assertions pertinentes, peuvent être jugées importantes par l'auditeur, comprennent des informations à fournir sur :

- Les liquidités ou les clauses restrictives dans les contrats de prêt, lorsque l'entité éprouve des difficultés financières ;
- Les événements ou les circonstances qui ont mené à la comptabilisation d'une perte de valeur ;
- Les principales sources d'incertitude relative aux estimations, incluant les hypothèses d'avenir ;
- La nature d'un changement de méthode comptable et les autres informations pertinentes requises par le référentiel comptable applicable, lorsque, par exemple, l'on s'attend à ce que les nouvelles obligations d'information financière aient une incidence importante sur la situation financière de l'entité et sur sa performance financière ;
- Les accords de paiement fondé sur des actions, notamment les informations sur la manière dont les montants enregistrés ont été déterminés, et d'autres informations à fournir pertinentes ;
- Les parties liées et les transactions entre parties liées ;
- Les analyses de sensibilité, y compris les effets des changements dans les hypothèses retenues aux fins des techniques d'évaluation de l'entité, visant à permettre aux utilisateurs de comprendre l'incertitude relative à la mesure sous-jacente à un montant comptabilisé ou communiqué.

Évaluation des risques d'anomalies significatives au niveau des assertions

Évaluation du risque inhérent (Voir par. 31–33)

Évaluation de la probabilité et de l'ampleur des anomalies (Voir par. 31)

Raisons pour lesquelles l'auditeur évalue la probabilité et l'ampleur des anomalies

A205. L'auditeur évalue, pour chacun des risques d'anomalies significatives identifiés, la probabilité qu'une anomalie se produise et l'ampleur qu'elle pourrait prendre, le cas échéant, parce que c'est l'importance de la combinaison de ces deux variables qui détermine où se situent ces risques sur l'échelle de risque inhérent, et que cette information aide l'auditeur à concevoir des procédures d'audit complémentaires pour répondre aux risques.

A206. L'évaluation du risque inhérent pour les risques d'anomalies significatives identifiés assiste également l'auditeur à identifier les risques importants en vue de leur donner les réponses spécifiques exigées par la norme ISA 330 et d'autres normes ISA.

A207. Les facteurs de risque inhérent influencent l'évaluation de l'auditeur de la probabilité et de l'ampleur des anomalies relatives aux risques d'anomalies significatives qu'il a identifiés au niveau des assertions. Plus un flux d'opérations, un solde de compte ou une information à fournir sont susceptibles de comporter des anomalies significatives, plus le risque inhérent est susceptible d'être évalué comme étant élevé. La prise en compte de la mesure dans laquelle les facteurs de risque inhérent influent sur la possibilité qu'une assertion comporte une anomalie assiste l'auditeur à évaluer adéquatement le risque inhérent, relatif aux risques d'anomalies significatives identifiés au niveau des assertions, et à concevoir des réponses plus précises pour y répondre.

Échelle de risque inhérent

A208. Lors de son évaluation du risque inhérent, l'auditeur exerce son jugement professionnel pour déterminer l'importance de la combinaison que forment la probabilité et l'ampleur d'une anomalie.

A209. L'évaluation du risque inhérent relative à un risque d'anomalies significatives donné au niveau des assertions consiste à juger où se situe le risque sur l'échelle de risque inhérent, dans une fourchette allant de « faible » à « élevé ». 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.

- A210. Pour déterminer la probabilité d'une anomalie, l'auditeur prend en considération la possibilité que cette anomalie se produise, compte tenu des facteurs de risque inhérent.
- A211. Pour déterminer l'ampleur d'une anomalie potentielle, l'auditeur prend en considération ses aspects qualitatifs et quantitatifs (c'est-à-dire que les anomalies dans des assertions concernant des flux d'opérations, des soldes de comptes ou des informations à fournir peuvent être jugées significatives en raison de leur ordre de grandeur, de leur nature ou des circonstances).
- A212. L'auditeur se réfère à l'importance de la combinaison que forment la probabilité et l'ampleur d'une anomalie potentielle pour déterminer où se situe le risque inhérent sur l'échelle de risque inhérent (c'est-à-dire à l'intérieur de la fourchette). Plus l'importance de cette combinaison est élevée, plus le risque inhérent sera évalué comme étant élevé ; plus elle est faible, plus le risque inhérent sera évalué comme étant faible.
- A213. Pour qu'un risque soit évalué comme étant élevé sur l'échelle de risque inhérent, il n'est pas nécessaire que l'anomalie ait à la fois une grande ampleur et une probabilité élevée selon l'évaluation que fait l'auditeur. C'est plutôt le point d'intersection de l'ampleur et de la probabilité de l'anomalie significative qui détermine où se situe le risque inhérent sur l'échelle de risque inhérent (risque élevé ou faible). Différentes combinaisons de probabilité et d'ampleur peuvent donc donner lieu à un risque inhérent élevé (par exemple, une faible probabilité, combinée à une très grande ampleur, peut donner lieu à un risque élevé).
- A214. Afin de développer des stratégies appropriées en réponse aux risques d'anomalies significatives, l'auditeur peut, d'après son évaluation du risque inhérent, désigner les risques d'anomalies significatives en fonction de catégories sur l'échelle de risque inhérent. Ces catégories peuvent être établies de différentes manières. Quel que soit le type de catégorie utilisé, l'évaluation du risque inhérent par l'auditeur est appropriée lorsque la conception et la mise en œuvre de procédures d'audit complémentaires en réponse aux risques d'anomalies significatives identifiés au niveau des assertions prennent adéquatement en compte cette évaluation du risque inhérent et les raisons qui la sous-tendent.

Risques d'anomalies significatives diffus au niveau des assertions (Voir par. 31(b))

- A215. Lorsque l'auditeur procède à l'évaluation des risques d'anomalies significatives qu'il a identifiés au niveau des assertions, il peut conclure que certains des risques d'anomalies significatives concernent de manière plus diffuse les états financiers dans leur ensemble et qu'ils sont susceptibles d'affecter de nombreuses assertions, auquel cas l'auditeur peut revoir l'identification des risques d'anomalies significatives au niveau des états financiers.
- A216. Lorsque les risques d'anomalies significatives sont identifiés au niveau des états financiers en raison de leur effet diffus sur plusieurs assertions, et qu'ils peuvent être associés à des assertions précises, l'auditeur est tenu de prendre en compte ces risques dans son évaluation du risque inhérent relative aux risques d'anomalies significatives au niveau des assertions.

Considérations propres aux entités du secteur public

- A217. Lorsqu'il exerce son jugement professionnel pour évaluer les risques d'anomalies significatives, l'auditeur d'une entité du secteur public peut tenir compte de la complexité des textes réglementaires et des directives ainsi que des risques de non-respect de ces textes vis-à-vis des autorités.

Risques importants (Voir par. 32)

Raisons pour lesquelles l'auditeur identifie les risques importants et leur incidence sur l'audit

A218. L'identification des risques importants permet à l'auditeur d'accorder une plus grande attention aux risques qui se situent dans la partie supérieure de l'échelle, grâce à la mise en œuvre de certaines réponses requises. Par exemple :

- le paragraphe 26(a)(i) requiert de l'auditeur qu'il identifie les contrôles visant à répondre à des risques importants, et le paragraphe 26(d) requiert qu'il détermine si ces contrôles ont été conçus efficacement et mis en œuvre ;
- la norme ISA 330 requiert de l'auditeur qu'il teste les contrôles liés aux risques importants dans la période sur laquelle porte sa mission (s'il a l'intention de s'appuyer sur l'efficacité du fonctionnement de ces contrôles), et qu'il planifie et mette en œuvre des contrôles de substance répondant spécifiquement aux risques importants identifiés⁵² ;
- la norme ISA 330 requiert de l'auditeur qu'il recueille des éléments probants d'autant plus convaincants que, selon son évaluation, le risque est considéré comme élevé⁵³ ;
- la norme ISA 260 (révisée) requiert de l'auditeur qu'il communique aux personnes constituant le gouvernement d'entreprise les risques importants qu'il a identifiés⁵⁴ ;
- la norme ISA 701 requiert de l'auditeur qu'il prenne en considération les risques importants dans sa détermination des questions ayant nécessité une attention importante de sa part et qui peuvent donc constituer des points clés de l'audit⁵⁵ ;
- la revue de la documentation de l'audit par l'associé responsable de la mission, à des stades appropriés au cours de l'audit, permet la résolution en temps opportun des points importants, notamment des risques importants, au plus tard à la date du rapport de l'auditeur, à la satisfaction de l'associé responsable de la mission⁵⁶ ;
- la norme ISA 600 requiert une plus grande intervention de la part de l'associé responsable de l'audit du groupe si un risque important a été identifié au niveau d'un composant du groupe, et requiert également que l'équipe affectée à l'audit du groupe dirige les travaux à réaliser à l'égard du composant par l'auditeur du composant⁵⁷.

Identification des risques importants

A219. Pour identifier les risques importants, l'auditeur peut d'abord identifier les risques d'anomalies significatives évalués comme étant élevés sur l'échelle de risque inhérent, ce qui lui fournira une base pour déterminer ceux qui peuvent se situer près de l'extrémité supérieure de l'échelle. « Être près de l'extrémité supérieure de l'échelle de risque inhérent » diffèrera d'une entité à l'autre, et pas nécessairement identique d'une période à l'autre pour une même entité. Elle peut dépendre de la nature et des circonstances de l'entité pour laquelle le risque est évalué.

A220. L'identification des risques d'anomalies significatives qui, selon l'évaluation de l'auditeur, se situent près de l'extrémité supérieure de l'échelle de risque inhérent et qui, par conséquent, sont des risques importants, relève du jugement professionnel, à moins qu'il ne s'agisse d'un type de risque pour lequel il est précisé qu'il doit être traité comme un risque important conformément aux diligences d'une autre norme ISA. La norme ISA 240 contient d'autres diligences et indications concernant l'identification et l'évaluation des risques d'anomalies significatives résultant de fraudes⁵⁸.

⁵² Norme ISA 330, paragraphes 15 et 21

⁵³ Norme ISA 330, paragraphe 7(b)

⁵⁴ Norme ISA 260 (révisée), paragraphe 15

⁵⁵ Norme ISA 701, *Communication des questions clés de l'audit dans le rapport de l'auditeur indépendant*, paragraphe 9

⁵⁶ Norme ISA 220 (révisée), paragraphes 17 et A19

⁵⁷ Norme ISA 600, paragraphes 30–31

⁵⁸ Norme ISA 240, paragraphes 26–28.

Exemples :

- Pour une chaîne de supermarchés, la trésorerie sera normalement considérée comme un poste présentant une probabilité élevée d'anomalie en raison du risque de détournement, mais l'ampleur de l'anomalie potentielle sera généralement très faible, car les établissements gardent peu d'argent en espèces. Il est peu probable que la combinaison de ces deux facteurs sur l'échelle de risque inhérent amène l'auditeur à considérer que l'existence de la trésorerie présente un risque important.
- Une entité mène des négociations en vue de la vente de l'une de ses branches d'activité. Après avoir analysé l'incidence de cette vente sur la dépréciation du goodwill, l'auditeur peut déterminer l'existence d'une probabilité élevée d'anomalie et que l'ampleur que pourrait prendre l'anomalie est grande, compte tenu des facteurs de risque inhérent que sont la subjectivité, l'incertitude et la possibilité d'un biais introduit par la direction ou d'autres facteurs de risque de fraude. Il peut alors déterminer que la dépréciation du goodwill présente un risque important.

A221. L'auditeur prend également en compte l'incidence relative des facteurs de risque inhérent dans son évaluation du risque inhérent. Plus l'incidence des facteurs de risque inhérent est faible, plus il est probable que le risque sera évalué comme étant faible. Les risques d'anomalies significatives pouvant être considérés comme présentant un risque inhérent plus élevé – et, donc, être identifiés comme des risques importants – peuvent découler notamment des éléments suivants :

- les opérations pour lesquelles il existe de multiples traitements comptables acceptables, ce qui donne lieu à une certaine subjectivité ;
- les estimations comptables qui présentent un degré élevé d'incertitude d'estimation ou qui nécessitent l'utilisation de modèles complexes ;
- la complexité de la collecte et du traitement des données à l'appui des soldes de comptes ;
- les soldes de comptes ou les informations quantitatives qui nécessitent des calculs complexes ;
- les principes comptables qui peuvent faire l'objet d'interprétations différentes ;
- des changements survenus dans les activités de l'entité qui amènent des changements de traitements comptables, comme les fusions et acquisitions.

Risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés (Voir par. 33)

Raisons pour lesquelles l'auditeur doit identifier les risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés

A222. Dans certaines circonstances, en raison de la nature d'un risque d'anomalies significatives et des activités de contrôle visant à répondre à ce risque, il se peut que la seule façon de recueillir des éléments probants suffisants et appropriés soit de tester l'efficacité du fonctionnement des contrôles. L'auditeur est donc tenu d'identifier de tels risques en raison de leurs conséquences sur les procédures d'audit complémentaires à concevoir et à mettre en œuvre, conformément à la norme ISA 330, en réponse aux risques d'anomalies significatives au niveau des assertions.

A223. Le sous-paragraphe 26 (a)(iii) requiert également l'identification des contrôles visant à répondre aux risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés, étant donné que l'auditeur doit, conformément à la norme ISA 330⁵⁹, concevoir et mettre en œuvre des tests sur ces contrôles.

⁵⁹ Norme ISA 330, paragraphe 8

Identification des risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés

A224. Lorsque les opérations courantes relatives aux activités sont soumises à un processus de traitement fortement automatisé, avec peu ou pas d'intervention manuelle, il peut ne pas être possible d'effectuer seulement des contrôles de substance se rapportant au risque. Ceci peut être le cas dans des circonstances où une masse importante d'informations est initiée, enregistrée, traitée et présentée seulement sous une forme électronique ; tel est le cas dans un système intégré. Dans cette situation:

- Les éléments probants peuvent être disponibles seulement sous une forme électronique et leur caractère suffisant et approprié dépend de l'efficacité des contrôles sur leur exactitude et leur exhaustivité ;
- La probabilité que des informations soient générées ou modifiées de façon incorrecte et que ceci ne soit pas détecté est plus grande si des contrôles appropriés ne fonctionnent pas de manière efficace.

Exemple :

Des contrôles de substance ne peuvent généralement pas fournir à eux seuls des éléments probants suffisants et appropriés sur les produits d'une entité de télécommunications. En effet, il n'existe pas d'éléments probants sous une forme observable sur les appels effectués ou les données transmises. Habituellement, de nombreux tests de procédures sont plutôt effectués pour confirmer que la durée des appels et la transmission des données sont correctement saisies (par exemple en minutes ou en volume de téléchargement) et enregistrées dans le système de facturation de l'entité.

A225. La norme ISA 540 (révisée) fournit des modalités d'application supplémentaires sur les estimations comptables concernant les risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés⁶⁰. Dans le cas des estimations comptables, ces risques peuvent être liés non seulement au traitement automatisé, mais aussi aux modèles complexes.

Évaluation du risque lié au contrôle interne (Voir par. 34)

A226. Le fait que l'auditeur prévoie de tester l'efficacité du fonctionnement des contrôles internes dépend de ses attentes quant au fonctionnement efficace de ces contrôles internes et lui fournit une base pour évaluer le risque lié au contrôle interne. Les attentes initiales de l'auditeur quant à l'efficacité du fonctionnement des contrôles sont fondées sur son évaluation de la conception des contrôles identifiés de la composante « mesures de contrôle » et sa vérification de leur mise en œuvre. L'auditeur pourra confirmer ces attentes initiales après avoir testé l'efficacité du fonctionnement des contrôles conformément à la norme ISA 330. Si, contrairement aux attentes, les contrôles ne fonctionnent pas efficacement, il faudra que l'auditeur révise son évaluation du risque lié au contrôle interne, conformément au paragraphe 37.

A227. L'évaluation par l'auditeur du risque lié au contrôle interne peut s'effectuer de différentes façons, en fonction des techniques ou des méthodologies d'audit qu'il privilégie, et peut être reflétée de différentes manières.

A228. Lorsque l'auditeur prévoit de tester l'efficacité du fonctionnement des contrôles, il peut être nécessaire qu'il teste une combinaison de contrôles pour confirmer ses attentes à l'égard du fonctionnement efficace des contrôles. L'auditeur peut prévoir de tester des contrôles directs et indirects, y compris des contrôles généraux informatiques, et, le cas échéant, tenir compte de leur incidence combinée attendue lorsqu'il évalue le risque lié au contrôle interne. Lorsque le contrôle qui sera testé ne répond que partiellement au risque inhérent évalué, l'auditeur détermine les

⁶⁰ Norme ISA 540 (révisée), paragraphes A87–A89.

conséquences sur les procédures d'audit complémentaires à concevoir pour ramener le risque d'audit à un niveau suffisamment faible.

A229. Lorsque l'auditeur prévoit de tester l'efficacité du fonctionnement d'un contrôle automatisé, il peut également prévoir de tester l'efficacité du fonctionnement des contrôles généraux informatiques pertinents qui favorisent le fonctionnement continu de ce contrôle automatisé pour répondre aux risques provenant du recours à l'informatique et pour fonder son attente à l'égard du fonctionnement efficace du contrôle automatisé tout au long de la période. Lorsque l'auditeur s'attend à ce que les contrôles généraux informatiques pertinents soient inefficaces, cela peut avoir une incidence sur son évaluation du risque lié au contrôle interne au niveau des assertions, et il peut être nécessaire que les procédures d'audit complémentaires comprennent des contrôles de substance pour répondre aux risques provenant du recours à l'informatique qui sont applicables. La norme ISA 330 fournit des indications supplémentaires concernant les procédures que l'auditeur peut mettre en œuvre dans ces circonstances⁶¹.

Évaluation des éléments probants recueillis au moyen des procédures d'évaluation des risques (Voir par. 35)

Raisons pour lesquelles l'auditeur évalue les éléments probants recueillis au moyen des procédures d'évaluation des risques

A230. Les éléments probants recueillis au moyen des procédures d'évaluation des risques procurent à l'auditeur une base pour l'identification et l'évaluation des risques d'anomalies significatives – base sur laquelle il s'appuie pour concevoir des procédures d'audit complémentaires dont la nature, le calendrier et l'étendue sont fonction de son évaluation des risques d'anomalies significatives au niveau des assertions, conformément à la norme ISA 330. Par conséquent, les éléments probants recueillis au moyen des procédures d'évaluation des risques procurent une base pour 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.

Évaluation des éléments probants

A231. Les éléments probants recueillis au moyen des procédures d'évaluation des risques comprennent à la fois les informations qui étayent et corroborent les assertions de la direction et les informations qui les contredisent⁶².

Esprit critique

A232. Lors de son évaluation des éléments probants recueillis au moyen des procédures d'évaluation des risques, l'auditeur se demande s'il a acquis une connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité qui est suffisante pour lui permettre d'identifier les risques d'anomalies significatives, et s'il existe des éléments probants contradictoires, ce qui pourrait révéler l'existence d'un risque d'anomalies significatives.

Flux d'opérations, soldes de comptes et informations à fournir qui, sans être importants, sont significatifs (Voir par. 36)

A233. Comme expliqué dans la norme ISA 320⁶³, le caractère significatif et le risque d'audit sont pris en considération lors de l'identification et de l'évaluation des risques d'anomalies significatives dans les flux d'opérations, les soldes de comptes et les informations à fournir. La détermination d'un seuil de signification relève du jugement professionnel de l'auditeur et est influencée par sa perception des

⁶¹ Norme ISA 330, paragraphes A29–A30.

⁶² Norme ISA 500, paragraphe A1.

⁶³ Norme ISA 320, paragraphe A1.

besoins d'information financière des utilisateurs des états financiers⁶⁴. Aux fins de l'application de la présente norme ISA et du paragraphe 18 de la norme ISA 330, les flux d'opérations, soldes de comptes et informations à fournir sont significatifs s'il est raisonnable de s'attendre à ce que leur omission, leur inexactitude ou le fait de les occulter puisse influencer les décisions économiques que les utilisateurs des états financiers prennent en se fondant sur les états financiers pris dans leur ensemble.

A234. Il peut exister des flux d'opérations, soldes de comptes ou informations à fournir qui, sans être des flux d'opérations importants, des soldes de comptes importants ou des informations à fournir importantes (c'est-à-dire qu'il n'y a pas d'assertions pertinentes identifiées), sont significatifs.

Exemple :

L'entité peut avoir fourni des informations sur la rémunération des dirigeants à l'égard desquelles l'auditeur n'a pas identifié de risque d'anomalies significatives. Toutefois, l'auditeur peut déterminer, en se fondant sur les considérations énoncées au paragraphe A233, que ces informations sont significatives.

A235. La norme ISA 330 traite des procédures d'audit à mettre en œuvre à l'égard des flux d'opérations, soldes de comptes et informations à fournir qui sont significatifs sans toutefois être considérés comme des flux d'opérations, soldes de compte ou information à fournir importants au sens du paragraphe 12(k),⁶⁵. Si l'auditeur détermine, en application du paragraphe 29, qu'un flux d'opérations, un solde de compte ou des informations à fournir sont importants, cette catégorie d'opérations, ce solde de compte ou ces informations à fournir sont significatifs aux fins de l'application du paragraphe 18 de la norme ISA 330.

Révision de l'évaluation des risques (Voir par. 37)

A236. Durant l'audit, il se peut que l'auditeur prenne connaissance de nouvelles informations ou d'autres informations qui diffèrent sensiblement des informations ayant servi à son évaluation des risques.

Exemple :

L'évaluation des risques de l'entité peut reposer sur l'attente du fonctionnement efficace de certains contrôles. En testant ces contrôles, l'auditeur peut recueillir des éléments probants indiquant que les contrôles ne fonctionnaient pas efficacement à des moments pertinents au cours de l'audit. De même, lors de la mise en œuvre de contrôles de substance, l'auditeur peut détecter des anomalies dont les montants ou la fréquence ne sont pas compatibles avec son évaluation des risques. Dès lors, l'évaluation initiale des risques ne reflète pas adéquatement la situation réelle de l'entité et les procédures d'audit complémentaires prévues peuvent ne pas être efficaces pour détecter les anomalies significatives. Les paragraphes 16 et 17 de la norme ISA 330 fournissent des indications supplémentaires concernant l'évaluation de l'efficacité du fonctionnement des contrôles.

Documentation (Voir par. 38)

A237. Dans le cas de missions récurrentes, certains éléments de la documentation d'audits antérieurs peuvent être réutilisés, après mise à jour au besoin pour refléter les changements survenus dans les activités ou les processus de l'entité.

A238. La norme ISA 230 mentionne notamment qu'il se peut qu'il n'existe pas de façon unique de documenter l'exercice de l'esprit critique, mais que la documentation de l'audit peut néanmoins démontrer que l'auditeur a fait preuve d'esprit critique⁶⁶. Par exemple, lorsque certains éléments probants recueillis au moyen des procédures d'évaluation des risques corroborent les assertions de la direction et que d'autres les contredisent, la documentation peut mentionner comment l'auditeur a

⁶⁴ Norme ISA 320, paragraphe 4.

⁶⁵ Norme ISA 330, paragraphe 18.

⁶⁶ Norme ISA 230, paragraphe A7.

évalué ces éléments probants. Elle peut inclure, y compris les jugements professionnels que l'auditeur a exercés pour évaluer si les éléments probants procurent une base appropriée pour son identification et son évaluation des risques d'anomalies significatives. D'autres exemples d'autres diligences de la présente norme ISA pour lesquelles la documentation peut attester que l'auditeur a fait preuve d'esprit critique comprennent :

- le paragraphe 13, qui requiert que l'auditeur conçoive et mette en œuvre les procédures d'évaluation des risques en évitant tout biais qui favoriserait l'obtention d'éléments probants corroborant l'existence de risques ou l'exclusion d'éléments probants contredisant l'existence de risques ;
- le paragraphe 17, qui requiert que les membres clés de l'équipe affectés à la mission s'entretiennent de l'application du référentiel comptable applicable ainsi que de la possibilité que les états financiers de l'entité comportent des anomalies significatives ;
- le paragraphe 19(b) et le paragraphe 20, qui requièrent que l'auditeur acquière une connaissance des raisons des changements dans les méthodes comptables retenues par l'entité et qu'il évalue si ces méthodes sont appropriées et conformes au référentiel comptable applicable ;
- les paragraphes 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) et le paragraphe 27, qui requièrent que l'auditeur évalue, après avoir acquis la connaissance requise, si les composantes du système de contrôle interne de l'entité sont appropriées aux circonstances de celle-ci, compte tenu de la nature et de la complexité de l'entité, et qu'il détermine si une ou plusieurs déficiences de contrôle ont été relevées ;
- le paragraphe 35, qui requiert que l'auditeur tienne compte de tous les éléments probants recueillis au moyen des procédures d'évaluation des risques, que ces éléments corroborent ou contredisent les assertions de la direction, et qu'il évalue si ces éléments probants procurent une base appropriée pour l'identification et l'évaluation des risques d'anomalies significatives ;
- le paragraphe 36, qui requiert que l'auditeur évalue si le jugement qu'il a porté en déterminant qu'il n'y avait pas de risques d'anomalies significatives relativement aux flux d'opérations, aux soldes de comptes et aux informations à fournir qui sont significatifs demeure approprié.

Application proportionnée

A239. La façon dont l'auditeur consigne dans son dossier les informations requises au paragraphe 38 relève de son jugement professionnel.

A240. Une documentation plus détaillée peut être requise – suffisante pour permettre à un auditeur expérimenté, n'ayant pas de lien antérieur avec la mission d'audit, de comprendre la nature, le calendrier et l'étendue des procédures d'audit réalisées – pour étayer les raisonnements motivant les jugements difficiles qui ont été portés.

A241. Dans le cas d'audits d'entités peu complexes, la forme et l'étendue de la documentation peuvent être simples et relativement succinctes. La forme et l'étendue de la documentation dépendent de la nature, de la taille et de la complexité de l'entité et de son système de contrôle interne, de l'information disponible auprès de l'entité ainsi que des méthodes et de la technologie employées au cours de l'audit. Il n'est pas nécessaire de consigner dans le dossier tous les aspects de la connaissance de l'entité acquise par l'auditeur et des questions qui s'y rattachent. Les éléments clés⁶⁷ de cette connaissance consignés par l'auditeur dans ses dossiers peuvent comprendre ceux sur lesquels il a fondé son évaluation des risques d'anomalies significatives. Toutefois, l'auditeur n'est pas tenu de consigner dans le dossier chaque facteur de risque inhérent pris en compte dans l'identification et l'évaluation des risques d'anomalies significatives au niveau des assertions.

⁶⁷ Norme ISA 230, paragraphe 8.

Exemple :

Dans le cas d'audits d'entités peu complexes, la documentation de l'audit peut être intégrée dans la documentation de l'auditeur sur la stratégie générale d'audit et le programme de travail⁶⁸. De même, par exemple, les résultats de l'évaluation des risques peuvent être consignés séparément ou être intégrés à la documentation de l'auditeur sur les procédures d'audit complémentaires⁶⁹.

⁶⁸ Norme ISA 300, *Planification d'un audit d'états financiers*, paragraphes 7, 9 et A11.

⁶⁹ Norme ISA 330, paragraphe 28.

Éléments à prendre en considération pour prendre connaissance de l'entité et de son modèle économique

La présente annexe décrit les objectifs et l'objet du modèle économique et contient des exemples d'éléments que l'auditeur peut prendre en considération pour prendre connaissance des activités de l'entité qui s'inscrivent dans un tel modèle. La connaissance du modèle économique de l'entité et de la manière dont celui-ci est influencé par la stratégie et les objectifs d'affaires peut aider l'auditeur à identifier les risques liés à l'activité qui peuvent avoir une incidence sur les états financiers. Elle peut également faciliter l'identification des risques d'anomalies significatives.

Objectifs et objet du modèle économique de l'entité

1. Le modèle économique décrit ce en quoi consistent, d'après l'entité, sa structure organisationnelle, son fonctionnement ou la portée de ses activités, ses branches d'activité (y compris les concurrents et les clients pour chacune de ces branches), de même que ses processus, ses possibilités de croissance, son degré de mondialisation, son cadre réglementaire et son utilisation des technologies. Il décrit comment l'entité s'y prend pour créer, préserver ou obtenir de la valeur financière ou autre pour ses parties prenantes.
2. Les stratégies sont les approches au moyen desquelles la direction prévoit d'atteindre les objectifs de l'entité, notamment la manière dont elle prévoit de répondre aux risques et de tirer profit des occasions qui se présentent. La direction les modifie au fil du temps afin de tenir compte des changements qui touchent ses objectifs ou les circonstances internes et externes de l'entité.
3. Le modèle économique décrit généralement :
 - la portée des activités de l'entité et les raisons pour lesquelles l'entité exerce ces activités ;
 - la structure de l'entité et l'ampleur de ses activités ;
 - les marchés ou les secteurs géographiques ou démographiques dans lesquels l'entité exerce ses activités, y compris le maillon de la chaîne de valeur dont elle fait partie, de même que la façon dont elle intervient dans ces marchés ou secteurs (principaux produits, segments de marché, méthodes de distribution) et ce qui la démarque de ses concurrents ;
 - les processus opérationnels ou les processus de fonctionnement de l'entité (en ce qui concerne, par exemple, les activités d'investissement, de financement ou d'exploitation), en mettant l'accent sur les aspects des processus opérationnels qui sont importants au regard de la création, de la préservation ou de l'obtention de valeur ;
 - les ressources (financières, humaines, intellectuelles, environnementales, technologiques ou autres) et autres intrants ou relations (clients, concurrents, fournisseurs, employés ou autres) qui sont essentiels ou importants pour sa réussite ;
 - la manière dont on a recours à l'informatique, dans ce modèle économique, pour permettre à l'entité d'interagir avec ses clients, ses fournisseurs, ses prêteurs et ses autres parties prenantes, que ce soit au moyen d'interfaces informatiques ou d'autres outils technologiques.
4. Un risque lié à l'activité peut avoir des conséquences immédiates sur le risque d'anomalies significatives pour des flux d'opérations, soldes de comptes et informations à fournir, tant au niveau des assertions qu'au niveau des états financiers. Par exemple, le risque lié à l'activité découlant d'une détérioration importante de la valeur marchande de biens immobiliers peut accroître le risque d'anomalies significatives relatif à l'assertion sur l'évaluation d'un prêteur qui consent des prêts à moyen terme garantis par des biens immobiliers. Cependant, le même risque peut avoir des conséquences à plus long terme, particulièrement lorsqu'il se conjugue avec une grave récession qui fait augmenter le risque sous-jacent de pertes de crédit pour la durée de vie des prêts. L'exposition au risque de pertes de crédit qui résulte de la combinaison de ces deux facteurs peut jeter un doute important sur la capacité de l'entité à poursuivre son exploitation, et cela peut avoir

une incidence sur les conclusions de la direction et de l'auditeur quant au caractère approprié de l'application par la direction du principe comptable de continuité d'exploitation et quant à l'existence ou non d'une incertitude significative. La question de savoir si un risque lié à l'activité peut donner lieu à un risque d'anomalies significatives est donc examinée à la lumière des circonstances propres à l'entité. Des exemples d'événements et de situations desquels peuvent découler des risques d'anomalies significatives sont présentés à l'**Annexe 2**.

Activités de l'entité

5. Exemples d'éléments que l'auditeur peut prendre en considération pour prendre connaissance des activités de l'entité (lesquelles s'inscrivent dans son modèle économique) :

(a) Activités de l'entité, telles que :

- Nature des sources de revenus, produits ou services, et débouchés, y compris le recours au e-commerce tel que les ventes par Internet et les modes de commercialisation;
- Conduite des activités (par exemple : étapes et modes de production, ou activités exposées à des risques environnementaux) ;
- Alliances, co-entreprises et activités de sous-traitance;
- Dispersion géographique et segmentation sectorielle ;
- Localisation des sites de production, des entrepôts, des bureaux et localisation et volume des stocks;
- Principaux clients et fournisseurs de marchandises ou prestataires de services, accords salariaux (y compris l'existence de conventions collectives, plans de retraite ou d'autres avantages postérieurs à l'emploi, stock-options ou accords de participation aux résultats, et réglementation gouvernementale relative aux questions salariales) ;
- Activités et dépenses de recherche et développement;
- Transactions avec des parties liées.

(b) Investissements et activités liées, telles que :

- Acquisitions ou désinvestissements planifiés ou récemment réalisés;
- Investissements ou cessions d'actions et de prêts;
- Prises de participation;
- Investissements dans des entités non consolidées, y compris les partenariats, les co-entreprises et les entités ad hoc.

(c) Financement et activités liées, telles que :

- Filiales et entités associées importantes, y compris les structures consolidées ou non consolidées;
- Structure et termes de l'endettement, y compris les accords de financement hors bilan et les contrats de leasing;
- Bénéficiaires économiques (nationaux, étrangers, leur réputation dans le monde des affaires et leur expérience), et parties liées;
- Recours à des instruments financiers dérivés.

Nature des entités ad hoc

6. Une entité ad hoc (quelquefois appelée « véhicule à but particulier ») est une entité qui est généralement créée dans un but circonscrit et bien défini, par exemple pour mettre en œuvre un bail, titriser des actifs financiers, ou pour mener des activités de recherche et développement. Elle peut prendre la forme d'une société, d'un trust, d'un partenariat ou d'une association de fait. L'entité pour le compte de laquelle l'entité ad hoc a été créée peut souvent transférer des actifs à cette dernière (par exemple, dans le cadre de la dématérialisation d'une transaction impliquant des actifs

financiers), obtenir le droit d'utiliser les actifs de l'entité qui les a transférés, ou rendre des services à celle-ci, tandis que d'autres parties peuvent lui fournir le financement. Comme la Norme ISA 550 l'indique, dans certaines situations, une entité ad hoc peut être une partie liée à l'entité⁷⁰.

7. Les référentiels comptables définissent souvent de manière détaillée les conditions qui apparaissent nécessaires pour assurer le contrôle, ou les circonstances dans lesquelles l'entité ad hoc doit entrer dans le périmètre de consolidation. L'interprétation des règles de ces référentiels comptables requiert souvent une connaissance détaillée des accords pertinents impliquant l'entité ad hoc.

⁷⁰ Norme ISA 550, paragraphe A7

Annexe 2

(Voir par. 12(f) et 19(c) et par. A7–A8, A85–A89)

Connaissance des facteurs de risque inhérent

La présente annexe donne des explications supplémentaires sur les facteurs de risque inhérent ainsi que sur les éléments que l'auditeur peut prendre en considération pour prendre connaissance des facteurs de risque inhérent et en tenir compte dans l'identification et l'évaluation des risques d'anomalies significatives au niveau des assertions.

Facteurs de risque inhérent

1. Les facteurs de risque inhérent sont les caractéristiques d'événements ou situations ayant une incidence sur la possibilité qu'une assertion portant sur un flux 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 prise en considération des contrôles. Parmi ces facteurs, qui peuvent être qualitatifs ou quantitatifs, il y a la complexité, la subjectivité, le changement, l'incertitude ou la possibilité d'anomalies résultant de biais introduit par la direction ou d'autres facteurs de risque de fraude⁷¹, dans la mesure où ils influent sur le risque inhérent. Lorsque, conformément aux paragraphes 19 (a)–(b), l'auditeur acquiert une connaissance de l'entité et de son environnement ainsi que du référentiel comptable applicable et des méthodes comptables retenues par l'entité, il acquiert aussi une connaissance de la façon dont les facteurs de risque inhérent influent, dans le cadre de la préparation des états financiers, sur la possibilité que les assertions comportent des anomalies.
2. Exemples de facteurs de risque inhérent qui concernent la préparation de l'information exigée par le référentiel comptable applicable (dans le présent paragraphe, cette information est désignée par l'expression « information exigée ») :
 - *Complexité* — La complexité découle de la nature de l'information exigée ou de la manière dont elle est préparée, notamment lorsque les processus entourant sa préparation présentent des difficultés inhérentes. Ainsi, il peut y avoir de la complexité, par exemple :
 - lorsqu'on calcule les provisions pour les remises accordées par des fournisseurs, car il faut parfois prendre en considération différentes modalités commerciales convenues avec un grand nombre de fournisseurs ou tenir compte de nombreuses modalités commerciales interreliées qui sont toutes pertinentes pour le calcul des remises à verser ;
 - lorsqu'on établit une estimation comptable pour laquelle il existe un grand nombre de sources de données possibles qui présentent chacune des caractéristiques différentes, et que le traitement de ces données comporte de nombreuses étapes liées, ce qui augmente les difficultés inhérentes à l'identification, à la saisie, à l'obtention, à la compréhension ou au traitement des données.
 - *Subjectivité* — Les contraintes inhérentes qui limitent la capacité de préparer l'information exigée avec objectivité, telles que le manque de connaissances ou d'informations, peuvent obliger la direction à faire un choix ou à porter des jugements subjectifs quant à l'approche qu'il convient d'adopter et aux informations à inclure dans les états financiers, ce qui implique une part de subjectivité. S'il y a plus d'une façon de préparer l'information exigée, on peut arriver à différents résultats tout en respectant les exigences du référentiel comptable applicable. Plus on manque de connaissances ou de données, plus la subjectivité des jugements pouvant être portés par des personnes raisonnablement bien informées et indépendantes augmente et plus l'éventail des résultats possibles est large.

⁷¹ Norme ISA 240, paragraphes A24–A27

- *Changement* — Le changement résulte d'événements ou de situations qui, avec le temps, ont une incidence sur les affaires de l'entité ou sur l'environnement dans lequel elle exerce ses activités, que ce soit sur le plan économique, comptable, réglementaire, sectoriel ou autre, et dont les effets sont reflétés dans l'information exigée. De tels événements ou situations peuvent survenir au cours d'une période de présentation de l'information financière, ou entre deux périodes. Ainsi, les modifications apportées aux exigences du référentiel comptable applicable ou les faits nouveaux concernant l'entité et son modèle économique ou l'environnement dans lequel elle exerce ses activités peuvent donner lieu à des changements. Ces changements peuvent influencer sur les hypothèses ou les jugements de la direction, notamment en ce qui concerne le choix de méthodes comptables ou la façon dont les estimations comptables et les informations y afférentes sont préparées.
 - *Incertitude* — Il y a de l'incertitude lorsqu'il n'est pas possible de préparer l'information exigée en se fondant uniquement sur des données qui sont suffisamment précises et complètes et qui sont vérifiables au moyen d'une observation directe. Il est alors parfois nécessaire d'adopter une approche reposant sur les connaissances disponibles afin de préparer l'information exigée à l'aide de données observables suffisamment précises et complètes, dans la mesure où de telles données sont disponibles, et, lorsqu'elles ne le sont pas, au moyen d'hypothèses raisonnables qui sont étayées par les données disponibles les plus appropriées. Les contraintes qui limitent la disponibilité des connaissances ou des données et qui sont indépendantes de la volonté de la direction (sous réserve des contraintes de coût, le cas échéant) créent de l'incertitude et ont un effet inévitable sur la préparation de l'information exigée. Par exemple, lorsque le montant en numéraire exigé ne peut être déterminé avec précision et que le dénouement de l'estimation n'est pas connu avant la date de finalisation des états financiers, il y a de l'incertitude d'estimation.
 - *Possibilité d'anomalies résultant de biais introduit par la direction ou d'autres facteurs de risque de fraude, dans la mesure où ils influent sur le risque inhérent* — La possibilité d'anomalies résultant de biais introduit par la direction découle de situations pouvant amener la direction à manquer de neutralité, intentionnellement ou non, au moment de préparer l'information exigée. Les biais introduits par la direction sont souvent associés à des situations (indices d'un biais possible introduit par la direction) qui peuvent donner lieu à un manque de neutralité dans les jugements de la direction et, par conséquent, à une anomalie significative qui, si elle est intentionnelle, constitue une fraude. L'existence de motifs ou de pressions qui influent sur le risque inhérent (dont la volonté d'atteindre un objectif, comme un résultat net ou un ratio de fonds propres attendu) en incitant la direction à manquer de neutralité, et l'existence de circonstances favorables à un tel manque sont des exemples de tels indices. Les facteurs qui touchent plus précisément la possibilité d'anomalies résultant de fraudes associées à des informations financières mensongères et à des détournements d'actifs sont décrits aux paragraphes A1–A5 de la norme ISA 240.
3. Lorsque la complexité fait partie des facteurs de risque inhérent, on peut supposer que la direction devra utiliser des processus complexes pour préparer l'information, et que ceux-ci seront particulièrement difficiles à mettre en œuvre. Il se pourrait donc que des compétences et des connaissances spécialisées soient nécessaires et que la direction soit obligée d'avoir recours à un expert de son choix.
 4. Lorsque le jugement de la direction comporte une grande part de subjectivité, la possibilité d'anomalies résultant de biais, intentionnels ou non, introduits par la direction peut augmenter. Par exemple, lorsque la direction a dû porter des jugements importants pour établir des estimations comptables identifiées comme présentant un degré élevé d'incertitude d'estimation, il se peut que des biais, intentionnels ou non, se dégagent des conclusions de la direction quant aux méthodes, aux données et aux hypothèses à employer.

Exemples d'événements et de situations pouvant donner lieu à des risques d'anomalies significatives.

5. Le tableau ci-après donne des exemples d'événements (dont des opérations) et de situations pouvant indiquer l'existence de risques d'anomalies significatives dans les états financiers, au niveau des états financiers ou au niveau des assertions. Les exemples suivants, regroupés par facteur de risque inhérent, couvrent un large éventail d'événements et de situations, mais ne sont pas tous pertinents pour toutes les missions d'audit, et la liste des exemples n'est pas nécessairement exhaustive. Les événements et situations ont été classés en fonction du facteur de risque inhérent qui pourrait avoir la plus grande incidence dans les circonstances. Il est important de noter qu'en raison des relations entre les facteurs de risque inhérent, les événements et les situations donnés en exemple sont également susceptibles d'être touchés, à différents degrés, par d'autres facteurs de risque inhérent.

Facteur de risque inhérent	Exemples d'événements ou de situations pouvant indiquer l'existence de risques d'anomalies significatives au niveau des assertions
Complexité	<p>Réglementation :</p> <ul style="list-style-type: none"> • Activités soumises à une réglementation très complexe. <p>Modèle économique :</p> <ul style="list-style-type: none"> • Existence d'alliances complexes et de co-entreprises. <p>Référentiel comptable applicable :</p> <ul style="list-style-type: none"> • Évaluations comptables impliquant des processus complexes. <p>Opérations :</p> <ul style="list-style-type: none"> • Recours à des financements hors-bilan, entités ad hoc, et autres mécanismes complexes de financement.
Subjectivité	<p>Référentiel comptable applicable :</p> <ul style="list-style-type: none"> • Estimation comptable pour laquelle il existe un large éventail de critères d'évaluation possibles (par exemple, comptabilisation, par la direction, de l'amortissement ou des produits et des charges liés au secteur de la construction). • Sélection, par la direction, d'une technique ou d'un modèle pour l'évaluation d'actifs non courants, comme des immeubles de placement.
Changement	<p>Conjoncture économique :</p> <ul style="list-style-type: none"> • Activités menées dans des régions qui sont économiquement instables, par exemple, des pays avec des dévaluations monétaires importantes ou une économie fortement inflationniste. <p>Marchés :</p> <ul style="list-style-type: none"> • Activités exposées à des marchés volatils par exemple, le marché des contrats à terme). <p>Perte de clients :</p> <ul style="list-style-type: none"> • Problème de continuité d'exploitation ou de liquidités, y compris la perte de clients importants. <p>Modèle sectoriel :</p> <ul style="list-style-type: none"> • Changements dans le secteur d'activité dans lequel l'entité opère. <p>Modèle économique :</p> <ul style="list-style-type: none"> • Modifications dans la chaîne d'approvisionnements. • Développement ou offre de nouveaux produits ou services, ou diversification dans de nouvelles activités. <p>Situation géographique :</p> <ul style="list-style-type: none"> • Expansion vers de nouvelles localisations. <p>Structure de l'entité :</p> <ul style="list-style-type: none"> • Changements dans l'entité tels que des acquisitions ou des réorganisations importantes ou autres événements inhabituels. • Entités ou branches d'activité susceptibles d'être cédées.

Facteur de risque inhérent	Exemples d'événements ou de situations pouvant indiquer l'existence de risques d'anomalies significatives au niveau des assertions
	<p>Ressources humaines :</p> <ul style="list-style-type: none"> • Changements dans le personnel-clé, y compris le départ de dirigeants-clés. <p>Informatique :</p> <ul style="list-style-type: none"> • Changements dans l'environnement informatique. • Installation de nouveaux systèmes informatiques importants liés à l'élaboration de l'information financière. <p>Référentiel comptable applicable :</p> <ul style="list-style-type: none"> • Application de nouvelles normes comptables. <p>Capital :</p> <ul style="list-style-type: none"> • Nouvelles Restrictions sur la disponibilité du capital et du crédit <p>Réglementation :</p> <ul style="list-style-type: none"> • Ouverture d'enquêtes sur les opérations ou les résultats financiers de l'entité par les autorités de contrôle ou des organismes gouvernementaux. • Incidence de nouveaux textes législatifs visant la protection de l'environnement.
Incertitude	<p>Informations :</p> <ul style="list-style-type: none"> • Événements ou opérations pour lesquels il existe une incertitude importante dans leur évaluation, y compris des estimations comptables, et les informations à fournir les concernant. • Litiges en cours ou passifs éventuels, comme par exemple les garanties après-ventes, les garanties financières et les coûts de dépollution.
Possibilité d'anomalies résultant de biais introduit par la direction ou d'autres facteurs de risque de fraude, dans la mesure où ils influent sur le risque inhérent	<p>Informations :</p> <ul style="list-style-type: none"> • Occasions pour la direction et les employés de présenter des informations financières mensongères (par exemple, omission d'informations importantes dans les informations à fournir, ou fait de les occulter). <p>Transactions :</p> <ul style="list-style-type: none"> • Transactions importantes avec les parties liées. • Volume important d'opérations non courantes ou non systématiques, y compris les opérations inter-sociétés, ou les opérations associées à des montants significatifs de produits en fin de période. • Opérations enregistrées sur la base d'intentions de la direction, par exemple, le refinancement de la dette, la cession d'actifs ou la classification au bilan des valeurs mobilières de placement.

Autres événements ou situations pouvant indiquer l'existence de risques d'anomalies significatives au niveau des états financiers :

- Manque de personnel disposant d'une compétence appropriée en matière comptable ou pour l'établissement d'états financiers.
- Faiblesses de contrôle interne (notamment en ce qui concerne l'environnement de contrôle ainsi que les processus d'évaluation des risques et de suivi par l'entité), en particulier celles auxquelles la direction n'a pas remédié.
- Anomalies antérieures, historique d'erreurs ou volume important d'ajustements en fin de période.

Annexe 3

(Voir par. 12(m) et par. 21–26 et A90–A181)

Connaissance du système de contrôle interne de l'entité

1. Le système de contrôle interne de l'entité peut se refléter dans les manuels de politiques et procédures, les systèmes et les formulaires ainsi que l'information qui s'y trouve ; ce sont les gens qui le mettent en œuvre. Le système de contrôle interne est mis en œuvre par la direction, les personnes constituant le gouvernement d'entreprise et d'autres membres du personnel, selon la structure de l'entité. Selon les décisions de la direction, des personnes constituant le gouvernement d'entreprise ou d'autres membres du personnel et selon les exigences législatives ou réglementaires, le système de contrôle interne peut être appliqué au modèle d'exploitation de l'entité, à sa structure juridique, ou aux deux.
2. La présente annexe donne des explications supplémentaires sur les composantes et les limites du système de contrôle interne de l'entité, qui sont décrites au paragraphe 12(m) et aux paragraphes 21–26 et A90–A181, dans le contexte d'un audit d'états financiers.
3. Le système de contrôle interne comprend des aspects qui portent sur les objectifs de l'entité en matière d'information, notamment en matière d'information financière, mais aussi des aspects qui concernent les objectifs d'exploitation ou de conformité, s'ils sont pertinents pour l'information financière.

Exemple :

Les contrôles afférents à la conformité aux textes législatifs ou réglementaires peuvent être pertinents pour l'information financière s'ils sont utiles à la préparation, par l'entité, des informations à fournir dans les états financiers au sujet des passifs éventuels.

Composantes du système de contrôle interne de l'entité*Environnement de contrôle*

4. L'environnement de contrôle inclut les fonctions de gouvernement d'entreprise et de direction, ainsi que le comportement, le degré de sensibilisation et les mesures prises par les personnes constituant le gouvernement d'entreprise et la direction relatives au contrôle interne et à son importance dans l'entité. L'environnement de contrôle donne le ton dans une organisation, en sensibilisant les membres du personnel à la nécessité des contrôles et constitue l'assise sur laquelle repose le fonctionnement des autres composantes du système de contrôle interne.
5. Certains des éléments de l'environnement de contrôle d'une entité ont un effet diffus sur l'évaluation des risques d'anomalies significatives. Par exemple, la sensibilité d'une entité à la notion de contrôle est influencée de manière importante par les personnes constituant le gouvernement d'entreprise, dès lors que l'un de leurs rôles consiste à contrebalancer les pressions sur la direction en rapport avec l'élaboration de l'information financière qui peuvent être exercées par le marché ou provenir des modes de rémunération. L'efficacité dans la conception de l'environnement de contrôle au regard de la participation des personnes constituant le gouvernement d'entreprise est alors influencée par des facteurs tels que:
 - L'indépendance de ces personnes vis-à-vis de la direction et leur capacité à évaluer les actions de celle-ci;
 - Leur compréhension réelle des opérations relevant de l'activité de l'entité;
 - La mesure dans laquelle elles évaluent la conformité des états financiers présentés avec le référentiel comptable applicable, notamment si les états financiers fournissent les informations adéquates.
6. L'environnement de contrôle comporte les éléments suivants :

- (a) *La façon dont la direction s'acquitte de ses responsabilités, notamment en développant et en entretenant la culture de l'entité et en démontrant l'importance qu'elle attache à l'intégrité et aux valeurs éthiques.* L'efficacité des contrôles ne peut se placer au-dessus des valeurs d'intégrité et d'éthique des personnes qui les créent, les gèrent et en assurent le suivi. L'intégrité et le comportement éthique des individus sont le produit des normes d'éthique et de comportement de l'entité ou de codes de conduite, et de la façon dont elles sont communiquées (au travers d'explications relatives à ces politiques) et mises en œuvre dans la pratique (par exemple, les actions de la direction pour éliminer ou minimiser les incitations ou les tentations qui peuvent encourager le personnel à s'engager dans des actes malhonnêtes, illégaux ou contraires à l'éthique). La communication des politiques de l'entité concernant les valeurs d'intégrité et d'éthique peut comprendre la communication au personnel de normes de comportement au travers d'explications relatives à ces politiques, d'un code de conduite et en donnant l'exemple.
- (b) *La façon dont les personnes constituant le gouvernement d'entreprise, lorsqu'ils ne sont pas membres de la direction, démontrent leur indépendance par rapport à la direction et exercent une surveillance à l'égard du système de contrôle interne de l'entité.* La sensibilité d'une entité à la notion de contrôle est influencée par les personnes constituant le gouvernement d'entreprise. L'auditeur peut se demander, entre autres, s'il y a un nombre suffisant de personnes qui sont indépendantes de la direction et qui font preuve d'objectivité dans leurs évaluations et leurs prises de décisions, comment les personnes constituant le gouvernement d'entreprise identifient et assument leurs responsabilités de surveillance et s'ils conservent la responsabilité de la surveillance de la conception, de la mise en œuvre et de l'application, par la direction, du système de contrôle interne de l'entité. L'importance des responsabilités des personnes constituant le gouvernement d'entreprise est formalisée dans des codes de bonne pratique et autres textes législatifs et réglementaires ou dans des guides édités à leur attention. D'autres responsabilités qui incombent aux personnes constituant le gouvernement d'entreprise concernent la surveillance de la conception et du fonctionnement efficace des procédures d'alerte..
- (c) *La façon dont l'entité attribue les pouvoirs et les responsabilités en vue d'atteindre ses objectifs.* Exemples d'éléments pouvant être pris en considération :
- les postes clés en matière de pouvoirs et de responsabilités et les voies hiérarchiques appropriées ;
 - les politiques concernant les pratiques commerciales appropriées, les connaissances et l'expérience exigées du personnel clé et les ressources fournies pour l'exercice des fonctions attribuées ;
 - les politiques et des communications destinées à s'assurer que tout le personnel comprend les objectifs de l'entité, la façon dont leur action personnelle interagit et contribue à atteindre les objectifs, et envisage comment et pourquoi il pourra être tenu pour responsable.
- (d) *La façon dont l'entité s'assure de recruter, de perfectionner et de retenir des personnes qui sont compétentes et dont le profil est compatible avec les objectifs de l'entité.* Cela comprend les moyens par lesquels l'entité s'assure que les personnes concernées possèdent les connaissances et les compétences nécessaires pour accomplir les tâches propres au poste qu'elles occupent, telles que :
- des critères de recrutement des personnes les plus qualifiées – qui mettent l'accent sur la formation de base, l'expérience professionnelle, les réalisations passées, et l'indication d'un comportement intègre et éthique – démontrent l'attachement de l'entité à recruter des gens de compétence et de confiance;
 - des politiques de formation qui exposent les rôles et les responsabilités futurs et qui incluent des stages de formation et des séminaires illustrent les niveaux de performance et de comportement attendus; et

- Des évaluations périodiques révèlent la volonté de l'entité de faire évoluer les personnes qualifiées à des niveaux de responsabilités plus élevés.
- (e) *La façon dont l'entité demande aux personnes ayant des responsabilités concernant son système de contrôle interne de lui rendre compte sur l'atteinte des objectifs de ce système. Exemples d'éléments pouvant être pris en considération :*
- les mécanismes relatifs à la communication, à l'obligation de rendre compte des personnes ayant des responsabilités en matière de contrôle et à la prise de mesures correctives, au besoin ;
 - les mesures de la performance, les incitatifs et les récompenses à l'intention des responsables du système de contrôle interne de l'entité, y compris la façon dont on évalue ces mesures et dont on s'assure qu'elles demeurent pertinentes ;
 - l'incidence des pressions associées à l'atteinte des objectifs en matière de contrôle sur les responsabilités et les mesures de la performance des personnes concernées ;
 - les sanctions disciplinaires qui sont imposées, au besoin.

Le caractère approprié de ces éléments dépend de la taille de l'entité, de la complexité de sa structure et de la nature de ses activités.

Processus d'évaluation des risques par l'entité

7. Le processus d'évaluation des risques par l'entité est un processus itératif d'identification et d'analyse des risques qui menacent l'atteinte des objectifs de l'entité ; il constitue la base à partir de laquelle la direction et les personnes constituant le gouvernement d'entreprise déterminent les risques à gérer.
8. Pour les besoins de l'élaboration de l'information financière, le processus d'évaluation des risques de l'entité comprend la manière dont la direction identifie les risques liés à l'activité ainsi qu'à l'établissement d'états financiers préparés conformément au référentiel comptable suivi par l'entité, la manière d'apprécier leur importance, d'évaluer la probabilité de leur survenance et de décider des actions à prendre pour y répondre ainsi que de les gérer et d'en assurer le suivi. Par exemple, le processus d'évaluation des risques de l'entité peut s'intéresser à la façon dont cette dernière prend en compte la possibilité d'opérations non enregistrées ou identifie et analyse des évaluations importantes incluses dans les états financiers.
9. Les risques concernant l'élaboration d'une information financière fiable proviennent d'événements externes et internes, d'opérations ou de circonstances qui peuvent survenir et compromettre la capacité d'une entité à initier, enregistrer, traiter et présenter des données financières conformes aux assertions de la direction sous-tendant les états financiers. La direction peut initier des plans, des programmes ou des actions pour répondre à des risques spécifiques ou peut décider d'assumer un risque en raison de coûts induits ou pour d'autres raisons. Les risques et leur évolution peuvent résulter de circonstances telles que:
 - *Changements dans l'environnement opérationnel. Les modifications de l'environnement réglementaire ou opérationnel peuvent modifier les pressions concurrentielles et créer des risques significativement différents ;*
 - *Personnel nouveau. Un nouveau personnel peut avoir une vision ou une compréhension différente du contrôle interne ;*
 - *Nouveaux systèmes d'information ou réorganisation des systèmes existants. Des changements importants et rapides dans les systèmes d'information peuvent modifier le risque afférent au contrôle interne ;*
 - *Croissance rapide. La croissance importante et rapide des activités peut peser fortement sur les contrôles et augmenter le risque de défaillance dans leur application ;*

- *Nouvelles technologies.* Le recours à de nouvelles technologies dans le processus de production ou dans les systèmes d'information peut modifier le risque lié au contrôle interne ;
- *Nouveaux modèles économique, produits ou activités.* L'entrée dans de nouveaux domaines d'activité ou types d'opérations avec lesquels l'entité a peu d'expérience peut entraîner de nouveaux risques liés au contrôle interne ;
- *Restructurations dans l'entité.* Les restructurations peuvent être accompagnées de réductions de personnel, de changements dans la supervision et dans la séparation des tâches qui peuvent modifier le risque lié au contrôle interne ;
- *Développement des activités à l'étranger.* L'extension ou l'acquisition d'activités à l'étranger fait naître des risques nouveaux et souvent uniques qui peuvent affecter le contrôle interne comme, par exemple, des risques additionnels ou différents relatifs aux opérations en devises ;
- *Nouvelles normes comptables.* L'adoption de nouveaux principes comptables ou la modification des principes comptables existants peuvent modifier les risques lors de l'établissement des états financiers.
- *le recours à l'informatique* — Risques concernant :
 - le maintien de l'intégrité des données et le traitement de l'information,
 - la stratégie d'entreprise de l'entité, si cette stratégie n'est pas soutenue efficacement par la stratégie informatique de l'entité,
 - la stabilité de l'environnement informatique de l'entité (changements ou interruptions) ou du personnel du service informatique (rotation du personnel), ou encore les mises à niveau nécessaires de l'environnement informatique (qui peuvent ne pas être effectuées en temps voulu, voire ne pas être effectuées du tout).

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

10. Le processus de suivi du système de contrôle interne par l'entité est un processus continu au moyen duquel l'entité évalue l'efficacité de son système de contrôle interne et prend les mesures correctives nécessaires en temps opportun. Il peut comporter des activités continues, des évaluations ponctuelles (réalisées périodiquement), ou une combinaison des deux. Ce suivi continu est souvent intégré aux activités normales récurrentes d'une entité et comprend les activités courantes d'encadrement et de supervision. L'étendue et la fréquence du processus varient généralement en fonction de l'évaluation des risques que fait l'entité.
11. Les objectifs et le champ de la fonction d'audit interne englobent généralement des activités d'assurance et de conseil conçues pour évaluer et assurer le suivi de l'efficacité du système de contrôle interne de l'entité⁷². Le processus de suivi de ce système par l'entité peut inclure des mesures telles que la revue par la direction de la préparation en temps voulu des rapprochements bancaires, de l'évaluation par les auditeurs internes du respect par le personnel commercial des politiques internes de l'entité concernant les clauses des contrats de ventes, et du contrôle exercé par le service juridique du respect des règles d'éthique de l'entité ou des politiques opérationnelles internes de celle-ci. Le suivi a également pour objectif de s'assurer que les contrôles continuent à fonctionner efficacement dans le temps. Par exemple, si la périodicité et l'exactitude des états de rapprochement bancaires ne sont pas surveillées, le personnel risque de cesser de les préparer.
12. Parmi les contrôles afférents au processus de suivi du système de contrôle interne par l'entité, y compris ceux qui assurent le suivi de contrôles sous-jacents automatisés, il peut y avoir des contrôles automatisés, des contrôles manuels, ou une combinaison des deux. Par exemple, pour assurer le suivi des accès à une technologie, une entité peut avoir recours à des contrôles automatisés (rapports générés automatiquement pour signaler toute activité inhabituelle à la direction) et à des contrôles manuels (investigation par la direction des exceptions relevées).

⁷² La « fonction d'audit interne » est décrite de façon plus détaillée dans la norme ISA 610 (révisée en 2013) et à l'Annexe 4 de la présente norme.

13. Pour faire la distinction entre une activité de suivi et un contrôle afférent au système d'information, il faut tenir compte des détails sous-jacents de l'activité, particulièrement si elle suppose la réalisation d'examens par des superviseurs. Ces examens ne sont pas considérés d'emblée comme des activités de suivi, et la question de savoir si un examen est considéré comme une activité de suivi ou comme un contrôle afférent au système d'information peut relever du jugement. Par exemple, le but d'un contrôle de l'exhaustivité mensuel est de détecter et de corriger des erreurs, tandis que celui d'une activité de suivi consiste à identifier la cause des erreurs et à confier à la direction la responsabilité de corriger le processus afin de prévenir d'autres erreurs. Autrement dit, un contrôle afférent au système d'information vise à répondre à un risque spécifique, tandis qu'une activité de suivi permet d'évaluer si les contrôles de chacune des cinq composantes du système de contrôle interne de l'entité fonctionnent comme prévu.
14. Le suivi des contrôles peut inclure l'utilisation d'une information venant de sources externes qui peut faire état de problèmes ou mettre l'accent sur les domaines nécessitant des améliorations. En réglant leurs factures, ou en les contestant, les clients corroborent ou non implicitement l'information concernant les facturations émises. De même, les autorités de contrôle peuvent communiquer avec l'entité sur des points qui concernent le fonctionnement du contrôle interne; par exemple, les communications relatives à des inspections faites par l'instance responsable du contrôle des banques. De même, la direction peut aussi prendre en considération dans son suivi des contrôles les communications des auditeurs externes sur son contrôle interne.

Système d'information et communications

15. Les aspects du système d'information qui sont pertinents pour la préparation des états financiers comprennent les activités et les politiques ainsi que les documents comptables et les documents justificatifs conçus pour et destinés à :
- initier, enregistrer et traiter les opérations de l'entité (et saisir, traiter et communiquer les informations sur les événements et les situations autres que les transactions) et à suivre les actifs, les passifs et les fonds propres qui leur sont liés;
 - résoudre les traitements incorrects des opérations, par exemple les fichiers automatisés de suspens et les procédures suivies pour apurer les écritures en suspens en temps voulu ;
 - suivre le processus et enregistrer les cas où le système a été contourné ou des contrôles outrepassés ;
 - incorporer dans le grand livre les informations résultant du traitement des opérations (en y transférant, par exemple, les opérations qui ont été accumulées dans les journaux auxiliaires) ;
 - saisir et traiter les informations pertinentes pour la préparation des états financiers concernant des faits ou des situations autres que des opérations, tels que les provisions et l'amortissement des actifs, et les changements dans le caractère recouvrable des comptes de tiers débiteurs;
 - s'assurer que l'information devant être fournie selon le référentiel comptable applicable est saisie, enregistrée, traitée, récapitulée et présentée de manière appropriée dans les états financiers.
16. Le processus opérationnel d'une entité désigne les mesures destinées à:
- développer, acheter, produire, vendre et distribuer les produits ou les services de l'entité ;
 - assurer la conformité des opérations avec les textes législatifs et réglementaires;
 - enregistrer l'information, y compris celle relative à la tenue de la comptabilité et à l'élaboration de l'information financière.

Le processus opérationnel donne lieu à des opérations qui sont enregistrées, traitées et présentées par le système d'information.

17. La qualité de l'information influe sur la capacité de la direction à prendre les décisions appropriées pour gérer et contrôler les activités de l'entité et pour présenter des informations financières fiables.
18. La communication, qui implique de faire connaître à chacun ses rôles et responsabilités respectifs en ce qui concerne le système de contrôle interne touchant à l'élaboration de l'information financière, peut prendre la forme de manuels de procédures, de manuels comptables et d'élaboration de l'information financière, et de notes écrites. La communication peut également se faire par voie électronique, orale et au travers des actions de la direction.
19. La communication, par l'entité, des rôles et des responsabilités concernant l'élaboration de l'information financière et des questions importantes la concernant, implique de faire connaître à chacun son rôle et sa responsabilité au regard du système de contrôle interne sur l'élaboration de cette information. Ceci peut comprendre des sujets tels que la compréhension par le personnel de la façon dont son rôle s'intègre dans le système d'élaboration de l'information financière par rapport aux autres et de la manière dont les exceptions sont communiquées à un niveau hiérarchique supérieur dans l'entité.

Mesures de contrôle

20. L'auditeur identifie les contrôles de la composante « mesures de contrôle » conformément au paragraphe 26. Ces contrôles comprennent des contrôles du traitement de l'information et des contrôles généraux informatiques, ces deux types de contrôles pouvant être manuels ou automatisés. Lorsqu'une grande proportion des contrôles concernant l'information financière auxquels la direction a recours ou sur lesquels elle s'appuie sont entièrement ou partiellement automatisés, il peut être d'autant plus important que l'entité mette en œuvre des contrôles généraux informatiques qui assurent le fonctionnement continu des éléments automatisés des contrôles du traitement de l'information. Les contrôles de la composante « mesures de contrôle » peuvent avoir trait aux éléments suivants :
 - *Autorisations et les approbations* — l'autorisation confirme qu'une opération est valide (c'est-à-dire qu'elle représente un événement économique réel ou qu'elle a été conclue conformément à une politique de l'entité). Elle revêt habituellement la forme d'une approbation par un dirigeant d'un échelon supérieur ou d'une vérification visant à établir la validité de l'opération. Un exemple du premier cas serait l'approbation par le superviseur d'une note de frais après examen du caractère raisonnable des frais engagés et de leur conformité à la politique de l'entité. La comparaison automatique du coût unitaire figurant sur la facture à celui qui figure sur le bon de commande et dont le résultat se situe sous le seuil de tolérance préalablement autorisé constitue un exemple d'approbation automatisée. Le traitement des factures dont l'écart se situe sous le seuil de tolérance est automatiquement approuvé. Les factures présentant un écart qui excède le seuil de tolérance sont signalées et font l'objet d'une investigation supplémentaire ;
 - *Rapprochements* — les rapprochements consistent à comparer deux ou plusieurs éléments de données. Lorsque des écarts sont relevés, des mesures sont prises afin de faire concorder les données. Les rapprochements visent généralement à assurer l'exhaustivité ou l'exactitude du traitement des opérations ;
 - *Vérifications* — les vérifications consistent à comparer deux ou plusieurs éléments les uns aux autres ou par rapport à une politique. Lorsque les éléments ne concordent pas ou qu'un élément n'est pas conforme à la politique, il est fort probable que des mesures de suivi soient prises. Les vérifications visent généralement à assurer l'exhaustivité, l'exactitude ou la validité du traitement des opérations ;
 - *Contrôles physiques ou logiques, y compris ceux qui assurent la sécurité des actifs contre un accès, une acquisition, une utilisation ou une cession non autorisée* — ces contrôles englobent :

- La sécurité physique des actifs, y compris les mesures de sauvegarde appropriées, telles que celles destinées à protéger les accès aux locaux et aux équipements pour sécuriser les actifs et les enregistrements,
- L'autorisation d'accès aux programmes informatiques et aux fichiers de données (c'est-à-dire l'accès logique),
- Les comptages périodiques et un rapprochement de ces derniers avec les chiffres figurant dans les états de contrôle (par exemple, la comparaison du comptage de caisse, du relevé du portefeuille titres ou des comptages de stocks avec la comptabilité);

La mesure dans laquelle des contrôles physiques mis en place et destinés à prévenir le détournement d'actifs sont pertinents pour l'établissement des états financiers dépend des circonstances, notamment lorsque des actifs sont fortement exposés à des détournements.

- *Séparation des tâches* — Elle vise à assigner à des personnes différentes la responsabilité de l'autorisation et de l'enregistrement des opérations, et d'assurer la surveillance des actifs. La séparation des tâches est destinée à réduire les occasions permettant à n'importe quelle personne d'être en position de perpétrer et de dissimuler des erreurs ou des fraudes dans le contexte normal de son travail.

Par exemple, il n'incombe pas au responsable de l'autorisation des ventes à crédit de tenir les registres des comptes clients ni de s'occuper des encaissements. Si la responsabilité de l'ensemble de ces activités était attribuée à une même personne, celle-ci pourrait, par exemple, créer une vente fictive pouvant ne pas être détectée. De même, les vendeurs ne devraient pas être en mesure de modifier les listes de prix des produits ni les taux de commission.

Il n'est pas toujours pratique, économique ou possible de séparer les tâches. Par exemple, les petites entités et les entités peu complexes peuvent ne pas disposer des ressources nécessaires pour séparer les tâches de façon idéale, et les coûts découlant de l'embauche de nouveaux employés peuvent être prohibitifs. En pareille situation, la direction peut mettre en œuvre d'autres contrôles. Dans l'exemple précédent, si le vendeur est en mesure de modifier les listes de prix des produits, une activité de contrôle de détection pourrait être effectuée périodiquement par des employés ne relevant pas de la fonction ventes afin de déterminer si le vendeur a modifié des prix et, le cas échéant, dans quelles circonstances.

21. Certains contrôles peuvent dépendre de l'existence de contrôles de supervision appropriés, établis par la direction ou les personnes constituant le gouvernement d'entreprise. Ainsi, certaines autorisations peuvent être déléguées dans le cadre de lignes directrices définies (par exemple, des critères d'investissement établis par les personnes constituant le gouvernement d'entreprise). Par contre, les opérations inhabituelles telles que les acquisitions et les désinvestissements importants peuvent nécessiter l'approbation spécifique d'un niveau hiérarchique supérieur, et même, dans certains cas, l'approbation des actionnaires.

Limites du contrôle interne

22. Le contrôle de son niveau d'efficacité, ne peut fournir à l'entité qu'une assurance raisonnable que ses objectifs, en matière d'élaboration de l'information financière, sont atteints. La possibilité d'atteindre ces objectifs est affectée par des limites inhérentes au contrôle interne. Ces limites incluent le fait que le jugement humain dans la prise de décision peut être erroné et que des manquements dans le contrôle interne peuvent survenir à cause d'une erreur humaine. Par exemple, il peut y avoir une erreur dans la conception d'un contrôle, ou lors de son changement. De la même façon, le fonctionnement d'un contrôle peut ne pas être efficace ; tel est le cas lorsqu'une information produite pour réaliser un contrôle interne (par exemple un rapport d'exceptions) n'est pas réellement utilisée parce que la personne responsable de la revue de cette information n'en comprend pas l'objectif ou ne prend pas les actions appropriées.

23. De plus, les contrôles peuvent être contournés suite à la collusion de deux personnes ou plus, ou le contrôle interne peut être outrepassé par la direction. Par exemple, la direction peut conclure des accords parallèles avec des clients qui viennent modifier les conditions générales de vente de l'entité, ce qui peut entraîner des erreurs dans la comptabilisation des produits. De même, des contrôles automatiques inclus dans les logiciels informatiques conçus pour identifier et signaler les opérations qui excèdent des limites de crédit spécifiques, peuvent être outrepassés ou neutralisés.
24. Enfin, en concevant et en mettant en place les contrôles, la direction peut exercer son jugement sur la nature et l'étendue des contrôles qu'elle souhaite voir mis en œuvre et sur la nature et l'étendue des risques qu'elle entend assumer.

Annexe 4

(Voir par. 14(a), par. 24(a)(ii), par. A25–A28 et par. A118)

Éléments à prendre en considération pour prendre connaissance de la fonction d'audit interne de l'entité

La présente annexe donne des exemples d'éléments que l'auditeur peut prendre en considération pour prendre connaissance de la fonction d'audit interne de l'entité (lorsque cette fonction existe).

Objectifs et étendue de la fonction d'audit interne

1. Les objectifs et le champ d'une fonction d'audit interne, la nature de ses attributions et sa position dans l'organisation, y compris ses pouvoirs et ses responsabilités, varient largement et dépendent de la taille et de la structure de l'entité, ainsi que des exigences de la direction et, le cas échéant, des personnes constituant le gouvernement d'entreprise. Ces points peuvent être indiqués dans une charte ou un cadre de référence de l'audit interne.
2. Les attributions d'une fonction d'audit interne peuvent inclure, par exemple, la mise en œuvre de procédures et l'évaluation de leurs résultats afin de fournir une assurance à la direction et aux personnes constituant le gouvernement d'entreprise quant à la conception et l'efficacité des processus de gestion des risques, de contrôle interne et de gouvernance. Le cas échéant, la fonction d'audit interne peut jouer un rôle important dans le suivi que fait l'entité du contrôle interne sur l'élaboration de l'information financière. Toutefois, les attributions de la fonction d'audit interne peuvent se concentrer principalement sur l'évaluation de la rentabilité, de l'efficacité et de l'efficacéité des opérations et, dans ce cas, les travaux de la fonction peuvent n'avoir aucun rapport direct avec l'élaboration de l'information financière de l'entité.

Demandes d'informations auprès de la fonction d'audit interne

3. Si une entité a une fonction d'audit interne, les demandes d'informations adressées aux personnes appropriées au sein de cette fonction peuvent fournir des renseignements utiles à l'auditeur pour sa prise de connaissance de l'entité et de son environnement, du référentiel d'information financière applicable et du système de contrôle interne de l'entité et pour l'identification et l'évaluation des risques d'anomalies significatives aux niveaux des états financiers et des assertions. Lors de la réalisation de ses travaux, la fonction d'audit interne a probablement obtenu des informations sur les activités de l'entité et les risques qui y sont liés, et peut avoir fait des constatations à partir de ses travaux, par exemple avoir identifié des déficiences dans le contrôle ou bien des risques, et ces constatations peuvent être d'une grande utilité pour l'auditeur dans sa prise de connaissance de l'entité et de son environnement, du référentiel d'information financière applicable et du système de contrôle interne de l'entité, dans son évaluation des risques et pour d'autres aspects de l'audit. L'auditeur procède donc à ces demandes d'informations, qu'il compte ou non s'appuyer sur les travaux de la fonction d'audit interne pour modifier la nature ou le calendrier des procédures d'audit à mettre en œuvre ou pour en réduire l'étendue. Des demandes d'informations particulièrement pertinentes peuvent porter sur des points soulevés par la fonction d'audit interne auprès des personnes constituant le gouvernement d'entreprise et sur les résultats de son propre processus d'évaluation des risques.
4. Si sur la base des réponses aux questions de l'auditeur, il apparaît que des constats sont susceptibles d'être pertinents par rapport à l'établissement de l'information financière de l'entité et à l'audit, l'auditeur peut considérer comme approprié de lire les rapports d'audit interne qui en traitent. Les rapports de la fonction d'audit interne qui peuvent être pertinents comprennent, par exemple, ses documents de stratégie et de planification et ses rapports préparés à l'intention de la direction ou des personnes constituant le gouvernement d'entreprise leur décrivant les constatations découlant des travaux d'audit interne.

5. En outre, conformément à la norme ISA 240, si la fonction d'audit interne fournit des renseignements à l'auditeur concernant des fraudes avérées, suspectées ou alléguées, l'auditeur en tient compte lors de son identification des risques d'anomalies significatives résultant de fraudes.
6. Les personnes appropriées au sein de la fonction d'audit interne auxquelles sont adressées les demandes d'informations sont celles qui, selon le jugement de l'auditeur, possèdent les connaissances, l'expérience et l'autorité voulues, par exemple le directeur de l'audit interne ou, selon les circonstances, d'autres membres du personnel au sein de la fonction. L'auditeur peut également considérer comme approprié de rencontrer périodiquement ces personnes.

Éléments de la fonction d'audit interne à prendre en considération pour comprendre l'environnement de contrôle

7. Pour prendre connaissance de l'environnement de contrôle, l'auditeur peut tenir compte des mesures prises par la direction à l'égard des constatations et des recommandations de la fonction d'audit interne concernant des déficiences de contrôle qui ont été relevées et qui sont pertinentes pour la préparation des états financiers, et notamment se demander si et comment ces mesures ont été mises en œuvre, et si elles ont été par la suite évaluées par la fonction d'audit interne.

Connaissance du rôle joué par la fonction d'audit interne dans le processus de suivi du système de contrôle interne par l'entité

8. Si la nature des attributions et des activités d'assurance de la fonction d'audit interne portent sur l'élaboration de l'information financière de l'entité, l'auditeur peut également être en mesure d'utiliser les travaux de la fonction d'audit interne pour modifier la nature ou le calendrier de ses propres procédures d'audit à mettre en œuvre pour recueillir des éléments probants, ou pour réduire l'étendue de ces procédures. L'auditeur peut être probablement plus enclin à utiliser les travaux de la fonction d'audit interne de l'entité si, par exemple, l'expérience des audits précédents ou les procédures d'évaluation des risques de l'auditeur semblent indiquer que la fonction d'audit interne de l'entité dispose de ressources adéquates et appropriées compte tenu de la taille de l'entité et de la nature de ses activités, et qu'elle relève directement des personnes constituant le gouvernement d'entreprise.
9. Si, compte tenu de sa prise de connaissance initiale de la fonction d'audit interne, l'auditeur envisage d'utiliser les travaux de la fonction d'audit interne pour modifier la nature ou le calendrier des procédures d'audit à mettre en œuvre ou pour en réduire l'étendue, la Norme ISA 610 (Révisée en 2013) s'applique.
10. Comme expliqué plus en détail dans la Norme ISA 610 (Révisée en 2013), les activités d'une fonction d'audit interne sont distinctes des autres contrôles de suivi susceptibles d'être pertinents pour l'élaboration de l'information financière, comme les revues de l'information comptable de la direction conçues pour contribuer à prévenir ou détecter des anomalies.
11. L'établissement de communications avec les personnes appropriées au sein de la fonction d'audit interne de l'entité suffisamment tôt dans la mission et le maintien de ces communications tout au long de la mission peuvent faciliter le partage efficace d'informations. Cela crée un environnement dans lequel l'auditeur peut être informé des points importants qui peuvent retenir l'attention de la fonction d'audit interne quand de tels points peuvent avoir une incidence sur les travaux de l'auditeur. La Norme ISA 200 explique l'importance pour l'auditeur de faire preuve d'esprit critique lors de la planification et de la réalisation de l'audit, ce qui implique d'être attentif aux informations qui remettent en question la fiabilité des documents et des réponses aux demandes d'informations devant servir d'éléments probants. Le maintien d'une communication avec la fonction d'audit interne tout au long de la mission peut donner aux auditeurs internes l'occasion d'attirer l'attention de l'auditeur sur de telles informations. L'auditeur peut alors en tenir compte dans son identification et son évaluation des risques d'anomalies significatives.

Annexe 5

(Voir par. 25(a), 26(b)–(c), A94, A166–A172)

Éléments à prendre en considération pour prendre connaissance du recours à l'informatique par l'entité

La présente annexe donne des exemples d'éléments que l'auditeur peut prendre en considération pour prendre connaissance de l'utilisation que fait l'entité de l'informatique dans son système de contrôle interne.

Connaissance du recours à l'informatique dans les composantes du système de contrôle interne de l'entité

1. Le système de contrôle interne de l'entité comprend des éléments manuels et automatisés (c'est-à-dire des contrôles et d'autres ressources manuels et automatisés qui sont utilisés dans le système de contrôle interne de l'entité). La proportion d'éléments automatisés par rapport aux éléments manuels varie selon la nature et la complexité de l'utilisation que fait l'entité de l'informatique. Le recours à l'informatique aura une incidence sur la manière dont l'entité traite, stocke et communique les informations pertinentes pour la préparation des états financiers conformément au référentiel comptable applicable et, par conséquent, sur la conception et la mise en œuvre de son système de contrôle interne. Chacune des composantes de ce système peut recourir à l'informatique dans une certaine mesure.

Généralement, un système informatique procure des avantages en termes d'efficacité du contrôle interne d'une entité en lui permettant:

- D'appliquer de manière permanente des règles prédéfinies touchant à son activité et de réaliser des calculs complexes en traitant un volume important d'opérations ou de données ;
 - D'améliorer les délais, la disponibilité et l'exactitude de l'information ;
 - De faciliter des analyses supplémentaires de l'information ;
 - D'améliorer la capacité à suivre la performance de ses activités ainsi que de ses politiques et procédures ;
 - De réduire le risque que les contrôles soient contournés ; et
 - D'augmenter la possibilité d'assurer de manière effective la séparation des tâches en mettant en œuvre des contrôles de sécurité dans les applications, les bases de données et les systèmes d'exploitation.
2. Les caractéristiques de ces éléments sont pertinentes pour l'évaluation des risques par l'auditeur et la définition des procédures d'audit complémentaires qui en résultent. Les contrôles automatisés peuvent se révéler plus fiables que les contrôles manuels, car ils sont susceptibles d'être moins facilement contournés, ignorés ou outrepassés, et sont aussi moins exposés à de simples erreurs ou fautes. Les contrôles automatisés peuvent être plus efficaces que les contrôles manuels dans les circonstances suivantes :
 - Volume important d'opérations ou opérations récurrentes, ou encore situations où des erreurs susceptibles d'être anticipées ou prévues peuvent être évitées, ou détectées et corrigées, grâce à l'automatisation ;
 - Mesures de contrôle où les moyens spécifiques d'exécution du contrôle peuvent être conçus et automatisés de manière adéquate.

Connaissance du recours à l'informatique dans le système d'information (Voir par. 25 (a))

3. Le système d'information de l'entité peut faire appel à des éléments manuels et des éléments automatisés ayant une incidence sur la façon dont les opérations sont initiées, enregistrées, traitées et communiquées. Plus précisément, les procédures d'initiation, d'enregistrement, de traitement et de communication des opérations peuvent se faire au moyen d'applications informatiques que l'entité

a configurées à ces fins. Par ailleurs, des documents électroniques peuvent venir remplacer ou compléter les documents papier.

4. Pour prendre connaissance des aspects de l'environnement informatique se rapportant au flux des opérations et au traitement de l'information dans le système d'information, l'auditeur recueille de l'information sur la nature et les caractéristiques des applications informatiques utilisées ainsi que de l'infrastructure informatique et des processus informatiques. Le tableau ci-après contient des exemples d'éléments que l'auditeur peut prendre en considération pour prendre connaissance de l'environnement informatique, en fonction de la complexité des applications informatiques utilisées au sein du système d'information de l'entité, et quelques caractéristiques typiques de chaque type d'environnement. Ces caractéristiques n'ont toutefois qu'une valeur indicative ; les caractéristiques propres à l'environnement informatique de l'entité peuvent différer selon la nature des applications informatiques particulières qu'utilise l'entité.

	Exemples de caractéristiques typiques		
	Logiciel disponible sur le marché peu complexe	Logiciel disponible sur le marché ou applications informatiques de moyenne envergure et modérément complexes	Applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés)
Éléments liés au degré d'automatisation et à l'utilisation des données			
<ul style="list-style-type: none"> Proportion de procédures de traitement qui sont automatisées et complexité de ces procédures (notamment, existence ou non de procédures de traitement sans papier hautement automatisées) 	N/A	N/A	Procédures automatisées poussées et souvent complexes
<ul style="list-style-type: none"> Mesure dans laquelle le traitement de l'information par l'entité repose sur des rapports générés par le système 	Rapports automatisés reposant sur une logique simple	Rapports automatisés reposant sur une logique simple, mais adaptée aux besoins	Rapports automatisés reposant sur une logique complexe ; utilisation d'un générateur de rapports
<ul style="list-style-type: none"> Méthode de saisie de données (saisie manuelle, saisie par le client ou par le fournisseur, ou téléchargement de fichiers, par exemple) 	Données saisies manuellement	Peu de données à saisir ou interfaces simples	Beaucoup de données à saisir ou interfaces complexes

<ul style="list-style-type: none"> Manière dont l'informatique est utilisée pour permettre la communication entre les applications, les bases de données ou d'autres éléments de l'environnement informatique, en interne ou à l'externe, selon le cas, grâce à des interfaces 	Aucune interface automatisée (saisie manuelle seulement)	Peu de données à saisir ou interfaces simples	Beaucoup de données à saisir ou interfaces complexes
<ul style="list-style-type: none"> Volume et complexité des données numériques traitées par le système d'information (notamment, stockage des documents comptables ou d'autres informations sous forme numérique ou non et lieu où les données sont stockées) 	Faible volume de données ou données simples pouvant être vérifiées manuellement ; stockage local des données	Faible volume de données ou données simples	Grand volume de données ou données complexes ; entrepôts de données ⁷³ ; recours à des fournisseurs de services informatiques internes ou externes (stockage ou hébergement des données par des tiers, par exemple)
Éléments liés aux applications informatiques et à l'infrastructure informatique			
<ul style="list-style-type: none"> Type d'applications (par exemple, applications commerciales peu ou pas personnalisées ou, au contraire, applications très personnalisées ou fortement intégrées, qui ont été soit achetées et personnalisées soit développées en interne) 	Applications commerciales peu ou pas personnalisées	Applications commerciales, applications développées en interne peu complexes, ou progiciel de gestion intégré d'entrée de gamme peu ou pas personnalisé	Applications développées sur mesure ou progiciels de gestion intégrés complexes et hautement personnalisés
<ul style="list-style-type: none"> Complexité de la nature des applications informatiques et de l'infrastructure informatique sous-jacente 	Simple ordinateur portable ou solution client-serveur	Ordinateur central bien établi et stable ; client-serveur petit ou simple ; logiciels en tant que services	Ordinateur central complexe ; client-serveur important ou complexe ; applications Web ; (infrastructure

⁷³ Un entrepôt de données s'entend généralement d'un référentiel central contenant des données intégrées qui proviennent d'une source unique ou de sources diverses (plusieurs bases de données, par exemple) et qui peuvent être utilisées pour la production de rapports ou pour d'autres activités d'analyse de données qu'effectue l'entité. Un générateur de rapports est une application informatique servant à extraire des données d'une ou de plusieurs sources (comme un entrepôt de données, une base de données ou une application informatique) et à les présenter selon un format défini.

		dans le Cloud (« SAAS Cloud »)	hébergée dans le Cloud)
<ul style="list-style-type: none"> Recours aux services d'hébergement de tiers ou externalisation des services informatiques 	Fournisseur compétent, bien établi et fiable pour les services externalisés (par exemple, fournisseur de solutions), le cas échéant	Fournisseur compétent, bien établi et fiable pour les services externalisés (par exemple, fournisseur de solutions), le cas échéant	Fournisseur compétent, bien établi et fiable pour certaines applications, et nouveau fournisseur ou fournisseur émergent pour d'autres
<ul style="list-style-type: none"> Recours à des technologies émergentes qui ont une incidence sur l'information financière de l'entité 	Pas d'utilisation de technologies émergentes	Utilisation limitée des technologies émergentes dans certaines applications	Utilisation mixte de technologies émergentes sur les différentes plateformes
Éléments liés aux processus informatiques			
<ul style="list-style-type: none"> Personnel qui s'occupe de l'environnement informatique (nombre de personnes faisant partie du personnel de soutien informatique chargé de la sécurité et de la gestion des changements dans l'environnement informatique, et niveau de compétence de ces personnes) 	Petit nombre de personnes ayant des connaissances limitées en informatique (mise à niveau des applications et gestion des accès)	Quelques personnes ayant des compétences en informatique / affectées aux technologies de l'information	Service consacré à l'informatique, doté de personnel qualifié possédant des compétences en programmation
<ul style="list-style-type: none"> Complexité des processus de gestion des droits d'accès 	Droits d'accès gérés par une seule personne détenant des droits d'administrateur	Droits d'accès gérés par un petit nombre de personnes détenant des droits d'administrateur	Droits d'accès gérés par le service informatique au moyen de processus complexes
<ul style="list-style-type: none"> Complexité des questions liées à la sécurité de l'environnement informatique, dont la vulnérabilité des applications informatiques, des bases de données et d'autres éléments de l'environnement informatique aux risques de cybersécurité, notamment lorsque des opérations sont 	Accès simple, sur place, sans éléments Web externes	Quelques applications Web sécurisées essentiellement par un simple contrôle d'accès en fonction du rôle	Plateformes multiples avec accès Web et modèles de sécurité complexes

effectuées au moyen du Web ou d'interfaces externes			
<ul style="list-style-type: none"> Modification des programmes liées à la manière dont l'information est traitée et, le cas échéant, ampleur des modifications apportées au cours de la période 	Logiciel disponible sur le marché dont le code source est inaccessible	Code source de certaines applications commerciales inaccessible, modifications légères ou peu nombreuses apportées à d'autres applications bien établies ; cycle de développement des systèmes traditionnel	Modifications nouvelles, nombreuses ou complexes ; plusieurs cycles de développement par année
<ul style="list-style-type: none"> Ampleur des changements survenus dans l'environnement informatique (par exemple, nouveautés dans cet environnement ou modifications importantes apportées aux applications informatiques ou à l'infrastructure informatique) 	Changements limités aux mises à niveau des logiciels commerciaux	Mises à niveau des logiciels commerciaux et des progiciels de gestion intégrés ou amélioration des applications ou systèmes patrimoniaux	Modifications nouvelles, nombreuses ou complexes ; plusieurs cycles de développement par année ; personnalisation importante des progiciels de gestion intégrés
<ul style="list-style-type: none"> Conversion de données majeure au cours de la période et, le cas échéant, nature et importance des changements apportés et méthode de conversion utilisée 	Mises à niveau logicielles provenant du fournisseur, sans conversion des données	Mises à niveau mineures pour les applications logicielles commerciales nécessitant peu de conversion de données	Mise à niveau majeure, nouvelle version, changement de plateforme

Technologies émergentes

5. L'entité peut utiliser des technologies émergentes (c.-à-d. les « blockchains », la robotique ou l'intelligence artificielle) parce qu'elles présentent des possibilités particulières d'accroître l'efficacité opérationnelle ou de renforcer l'information financière. Lorsque des technologies émergentes sont combinées au système d'information de l'entité utilisé pour la préparation des états financiers, l'auditeur peut les ajouter à la liste des applications informatiques et autres aspects de l'environnement informatique qui sont sujettes aux risques provenant du recours à l'informatique. Bien que les technologies émergentes puissent sembler plus sophistiquées ou plus complexes que les autres technologies, les responsabilités de l'auditeur à l'égard des applications informatiques et des contrôles généraux informatiques, décrites aux paragraphes 26 (b)–(c), demeurent les mêmes.

Application proportionnée

6. Il peut être plus facile pour l'auditeur de prendre connaissance de l'environnement informatique d'une entité peu complexe qui utilise un logiciel disponible sur le marché et qui, faute de pouvoir accéder au code source, ne peut apporter aucune modification aux programmes. Il est possible qu'une telle entité n'ait pas de personnel affecté au service informatique à proprement parler, mais qu'elle ait

attribué à un membre du personnel le rôle d'administrateur pour la gestion des droits d'accès des employés aux applications informatiques ou pour l'installation des mises à jour qu'envoie le fournisseur. Des éléments particuliers que l'auditeur peut prendre en considération pour prendre connaissance de la nature d'un progiciel comptable commercial, qui est parfois l'unique application informatique utilisée dans le système d'information d'une entité peu complexe comprennent :

- la mesure dans laquelle le logiciel est éprouvé et réputé pour sa fiabilité ;
- la mesure dans laquelle l'entité peut modifier le code source du logiciel pour ajouter des modules complémentaires au logiciel de base, ou modifier directement les données ;
- la nature et l'ampleur des modifications qu'a subies le logiciel. Il est possible que l'entité ne soit pas en mesure de modifier le code source du logiciel, mais qu'elle ait accès à des options de configuration (choix ou modification des paramètres de l'information, par exemple), celles-ci étant offertes par bon nombre de progiciels. Dans ce cas, le code source n'est généralement pas modifié, mais l'auditeur peut tout de même tenir compte de la gamme d'options de configuration que peut choisir l'entité lorsqu'il s'assure de l'exhaustivité et de l'exactitude des informations produites par le logiciel qui sont utilisées comme éléments probants ;
- la mesure dans laquelle il est possible d'accéder directement aux données pertinentes pour la préparation des états financiers (c'est-à-dire, d'accéder directement à la base de données sans passer par l'application informatique) et le volume de données traitées. Généralement, la nécessité pour l'entité de mettre en œuvre des contrôles visant à assurer l'intégrité des données (tels que des contrôles généraux informatiques prévenant l'accès – ou l'apport de modifications – non autorisé aux données) est d'autant plus grande que les données sont volumineuses.

7. Des environnements informatiques complexes peuvent inclure des applications informatiques qui, en raison de leur haut degré de personnalisation ou d'intégration, sont plus difficiles à comprendre. Les processus ou les applications informatiques se rapportant à l'information financière peuvent être intégrés à d'autres applications informatiques. Ainsi, il est possible que les applications informatiques utilisées pour le flux des opérations et le traitement de l'information dans le système d'information de l'entité reçoivent des données d'autres applications informatiques servant aux activités d'exploitation de l'entité. Ces autres applications peuvent alors être pertinentes pour la préparation des états financiers. Les environnements informatiques complexes nécessitent souvent un service consacré à l'informatique, doté de processus structurés et composé d'employés possédant des compétences en développement de logiciels et en maintenance d'environnement informatique. Il peut aussi arriver qu'une entité confie la gestion de certains aspects ou de certains processus de son environnement informatique à des fournisseurs de services internes ou externes (par exemple, en ayant recours aux services d'hébergement de tiers).

Identification des applications informatiques qui sont sujettes aux risques provenant du recours à l'informatique

8. En acquérant une connaissance de la nature et de la complexité de l'environnement informatique de l'entité, notamment de la nature et de l'étendue des contrôles du traitement de l'information, l'auditeur peut déterminer sur quelles applications informatiques s'appuie l'entité pour assurer l'exactitude du traitement et le maintien de l'intégrité de l'information financière. L'identification des applications informatiques sur lesquelles s'appuie l'entité peut influencer sur la décision de l'auditeur de tester ou non les contrôles automatisés qui y sont intégrés, dans la mesure où ils visent à répondre aux risques d'anomalies significatives identifiés. Si l'entité ne s'appuie pas sur une certaine application informatique, il est peu probable qu'il soit approprié ou concluant de tester l'efficacité du fonctionnement des contrôles automatisés qui y sont intégrés. Parmi les contrôles automatisés pouvant être identifiés en application du paragraphe 26 (b), il y a les calculs automatisés et les contrôles sur les données d'entrée, le traitement et les données de sortie, tels que le triple rapprochement (bons de commande, bordereaux d'expédition, factures). Lorsqu'il identifie de tels contrôles automatisés et que sa connaissance de l'environnement informatique l'amène à déterminer que l'entité s'appuie sur l'application informatique à laquelle ces contrôles sont intégrés, l'auditeur

peut être plus susceptible d'identifier cette application comme étant sujette aux risques provenant du recours à l'informatique.

9. Pour déterminer si les applications informatiques auxquelles sont intégrés les contrôles automatisés que l'auditeur a identifiés sont sujettes aux risques provenant du recours à l'informatique, l'auditeur tient généralement compte de la mesure dans laquelle la direction peut accéder au code source pour modifier les programmes liés à ces contrôles ou aux applications informatiques. La mesure dans laquelle l'entité modifie les programmes ou la configuration des applications informatiques et la mesure dans laquelle les processus informatiques afférents à ces modifications sont structurés peuvent aussi constituer des éléments pertinents à prendre en considération, tout comme le risque d'accès – ou d'apport de modifications – inapproprié aux données.
10. L'auditeur peut vouloir utiliser comme éléments probants des rapports générés par le système, tels que des balances âgées des créances clients ou des rapports d'évaluation des stocks. Afin de recueillir des éléments probants sur l'exhaustivité et l'exactitude de tels rapports, l'auditeur peut mettre en œuvre des contrôles de substance portant sur leurs données d'entrée et de sortie. Dans d'autres cas, il peut avoir l'intention de tester l'efficacité du fonctionnement des contrôles afférents à la préparation et la mise à jour de ces rapports, auquel cas l'application informatique qui génère les rapports fera probablement partie des applications sujettes aux risques provenant du recours à l'informatique. En plus de tester l'exhaustivité et l'exactitude des rapports, l'auditeur peut également prévoir de tester l'efficacité du fonctionnement des contrôles généraux informatiques visant à répondre aux risques de modification non autorisée ou inappropriée des programmes ou des données sous-tendant les rapports.
11. Une fonction de génération de rapports peut être intégrée dans l'application informatique, mais il se peut également que l'entité ait recours à une application distincte (générateur de rapports). Dans de tels cas, il peut être nécessaire de déterminer d'où proviennent les rapports générés par le système (c'est-à-dire de trouver l'application qui prépare les rapports ainsi que les sources de données utilisées) pour identifier les applications informatiques qui sont sujettes aux risques provenant du recours à l'informatique.
12. Les sources de données utilisées par les applications informatiques peuvent être des bases de données qui, par exemple, sont accessibles uniquement par l'intermédiaire de l'application informatique ou dont l'accès est restreint aux membres du personnel du service informatique qui détiennent des droits d'administrateur. Dans d'autres cas, la source de données peut être un entrepôt de données qui est lui-même considéré comme une application informatique sujette aux risques provenant du recours à l'informatique.
13. Lorsque l'entité a recours à des procédures sans papier hautement automatisées pour le traitement de ses opérations, ces procédures pouvant reposer sur de nombreuses applications informatiques intégrées, il est possible que l'auditeur identifie un risque pour lequel les contrôles de substance ne sont pas suffisants à eux seuls. Il y aura alors probablement des contrôles automatisés parmi les contrôles identifiés par l'auditeur. De plus, il se peut que l'entité s'appuie sur des contrôles généraux informatiques pour assurer le maintien de l'intégrité des opérations traitées et des autres informations servant au traitement. Les applications informatiques ayant un rôle dans le traitement et le stockage des informations feront alors probablement partie des applications sujettes aux risques provenant du recours à l'informatique.

Informatique utilisateur

14. Bien que l'auditeur puisse utiliser comme éléments probants des données générées par le système qui entrent dans les calculs effectués par un outil d'informatique utilisateur (comme un tableur ou une simple base de données), de tels outils ne figurent généralement pas parmi les applications informatiques identifiées en application du paragraphe 26 b). Il peut être difficile de concevoir et de mettre en œuvre des contrôles afférents à l'accès aux outils d'informatique utilisateur et à la

modification de ceux-ci, et de tels contrôles sont rarement équivalents aux contrôles généraux informatiques, ou aussi efficaces que ceux-ci. L'auditeur peut plutôt examiner une combinaison de contrôles du traitement de l'information, en tenant compte de l'objet et de la complexité de l'outil d'informatique utilisateur. telle que :

- les contrôles du traitement de l'information afférents à la production et au traitement des données sources, notamment les contrôles automatisés ou les contrôles d'interface pertinents jusqu'au point d'extraction des données (c'est-à-dire, l'entrepôt de données) ;
- les contrôles visant à assurer que la logique fonctionne comme prévu, notamment les contrôles qui concernent l'extraction des données, tels que le rapprochement d'un rapport et des données qui le sous-tendent, la comparaison des données individuelles d'un rapport aux données sources et vice versa ainsi que les contrôles relatifs aux formules et aux macros ;
- l'utilisation d'outils logiciels de validation, qui vérifient systématiquement les formules ou les macros (par exemple, outil validant l'intégrité d'une feuille de calcul).

Application proportionnée

15. La capacité de l'entité d'assurer le maintien de l'intégrité des informations qui sont stockées dans le système d'information, ou traitées au moyen de celui-ci, peut varier selon la complexité et le volume des opérations et des autres informations concernées. Si les données qui étayent un flux d'opérations important, un solde de compte important ou une information à fournir importante sont complexes et volumineuses, il sera d'autant plus difficile pour l'entité d'assurer le maintien de l'intégrité des informations en ayant seulement recours à des contrôles du traitement de l'information (par exemple, des contrôles sur les données d'entrée et de sortie ou des contrôles de revue). Il sera aussi moins probable que l'auditeur soit en mesure de recueillir des éléments probants sur l'exhaustivité et l'exactitude de ces informations, s'il compte se servir de ces informations comme éléments probants, en ayant seulement recours à des contrôles de substance. Parfois, lorsque les opérations sont peu complexes et peu volumineuses, la direction peut avoir recours à un contrôle du traitement de l'information qui permet à lui seul de vérifier l'exhaustivité et l'exactitude des données (par exemple, un rapprochement permettant de vérifier la concordance entre les bons de commande individuels qui ont été traités et pour lesquels il existe une facture et les informations se trouvant sur les documents papier d'où proviennent les données qui ont été saisies initialement dans l'application informatique). Lorsque l'entité s'appuie sur des contrôles généraux informatiques pour assurer le maintien de l'intégrité de certaines informations utilisées par les applications informatiques, l'auditeur peut déterminer que ces applications sont sujettes aux risques provenant du recours à l'informatique.

Exemples de caractéristiques propres aux applications informatiques qui sont généralement peu sujettes aux risques provenant du recours à l'informatique	Exemples de caractéristiques propres aux applications informatiques qui sont généralement sujettes aux risques provenant du recours à l'informatique
<ul style="list-style-type: none"> • Applications autonomes • Volume de données (opérations) peu important • Fonctionnalités peu complexes • Opérations systématiquement étayées par les originaux papier 	<ul style="list-style-type: none"> • Applications avec interfaces • Volume de données (opérations) important • Fonctionnalités complexes, telles que : <ul style="list-style-type: none"> ○ déclenchement automatique d'opérations ; ○ écritures automatisées basées sur un éventail de calculs complexes
Raisons pour lesquelles ces applications informatiques sont généralement peu sujettes aux risques provenant du recours à l'informatique :	Raisons pour lesquelles ces applications informatiques sont généralement sujettes aux risques provenant du recours à l'informatique :

<ul style="list-style-type: none"> • Le volume de données étant peu important, la direction ne s'appuie pas sur des contrôles généraux informatiques pour traiter ou tenir à jour les données. • La direction ne s'appuie pas sur des contrôles automatisés ni sur d'autres fonctionnalités automatisées. L'auditeur n'a pas identifié de contrôles automatisés en application du paragraphe 26 (a). • La direction ne s'appuie pas sur les rapports générés par le système, bien qu'elle les utilise à des fins de contrôle. Elle effectue plutôt un rapprochement entre la documentation papier et les rapports, dont elle vérifie aussi les calculs. • L'auditeur validera directement les informations produites par l'entité qui serviront d'éléments probants. 	<ul style="list-style-type: none"> • Le volume de données étant important, la direction s'appuie sur des logiciels d'application pour traiter ou tenir à jour les données. • La direction s'appuie sur des logiciels d'application pour effectuer des contrôles automatisés que l'auditeur a également identifiés.
--	--

Autres aspects de l'environnement informatique qui sont sujets aux risques provenant du recours à l'informatique

16. Lorsque des applications informatiques sont identifiées par l'auditeur comme étant sujettes aux risques provenant du recours à l'informatique, il existe généralement d'autres aspects de l'environnement informatique également sujettes à ces risques. L'infrastructure informatique se compose des bases de données, du système d'exploitation et du réseau. Les bases de données, qui peuvent consister en un ensemble de tables de données reliées, servent au stockage des données qui sont utilisées par les applications informatiques. Pour accéder directement aux données qui s'y trouvent, les membres du personnel du service informatique et les autres employés qui détiennent des droits d'administrateur peuvent avoir recours à des systèmes de gestion de base de données. Le système d'exploitation assure la gestion des communications entre le matériel, les applications informatiques et les autres logiciels qui sont utilisés dans le réseau. Il est ainsi possible que le système d'exploitation permette d'accéder directement aux applications informatiques et aux bases de données. Un réseau est une composante de l'infrastructure informatique qui permet la transmission de données et le partage d'informations, de ressources et de services grâce à une liaison de données commune. Un réseau comporte généralement des mesures de sécurité logique (dont l'exécution est assurée par le système d'exploitation) qui encadrent l'accès aux ressources sous-jacentes.
17. Généralement, lorsqu'une application informatique est identifiée par l'auditeur comme étant sujette aux risques provenant du recours à l'informatique, les bases contenant les données traitées par cette application sont elles aussi identifiées comme étant sujettes à ces risques. De même, le système d'exploitation est généralement sujet aux risques provenant du recours à l'informatique, puisqu'il est souvent essentiel au fonctionnement des applications informatiques et qu'il peut permettre d'accéder directement aux applications informatiques et aux bases de données. Le réseau peut être identifié comme étant sujet au risque lorsqu'il constitue un point d'accès central aux applications informatiques identifiées et aux bases de données connexes, lorsqu'une application informatique utilise Internet pour faciliter les interactions avec des fournisseurs ou des parties externes, ou lorsque des applications informatiques Web sont identifiées par l'auditeur.

Identification des risques provenant du recours à l'informatique et identification des contrôles généraux informatiques

18. Des exemples de risques provenant du recours à l'informatique comprennent les risques associés à un appui inapproprié sur des applications informatiques traitant de manière incorrecte des données, ou traitant des données incorrectes, voire les deux à la fois, tels que :
- L'accès non autorisé aux données pouvant entraîner la destruction des données ou leur modification inappropriée, y compris l'enregistrement d'opérations non autorisées, voire inexistantes, ou encore l'enregistrement incorrect des opérations. Des risques particuliers peuvent survenir lorsque des utilisateurs multiples accèdent à une base de données commune;
 - La possibilité pour le personnel du service informatique d'obtenir des accès privilégiés au-delà de ceux nécessaires à l'exercice de leur fonction, annihilant ainsi la séparation des tâches;
 - Des changements non autorisés de données dans des fichiers maîtres ;
 - Des changements non autorisés d'applications informatiques ou d'autres aspects de l'environnement informatique ;
 - Le fait de ne pas procéder aux changements nécessaires d'applications informatiques ou d'autres aspects de l'environnement informatique ;
 - Des interventions manuelles inappropriées;
 - La perte potentielle de données ou l'incapacité à accéder à certaines données tel qu'exigé.
19. Les risques pris en considération par l'auditeur concernant l'accès peuvent comprendre à la fois les risques d'accès non autorisé par des parties internes et les risques d'accès non autorisé par des parties externes (souvent appelés « risques liés à la cybersécurité »). Ces risques n'ont pas nécessairement d'incidence sur l'information financière vu que l'environnement informatique de l'entité peut également comprendre des applications informatiques et des données connexes répondant à d'autres besoins (exploitation ou conformité, par exemple). Il est important de noter que les cyber incidents surviennent généralement d'abord dans les couches internes et périphériques du réseau, habituellement à l'écart des applications informatiques, des bases de données et des systèmes d'exploitation qui ont une incidence sur la préparation des états financiers. Par conséquent, s'il prend connaissance d'une intrusion, l'auditeur détermine généralement la mesure dans laquelle celle-ci est susceptible d'avoir eu une incidence sur l'information financière. S'il est possible que l'intrusion ait eu une incidence sur l'information financière, l'auditeur peut décider de prendre connaissance des contrôles connexes et de tester ces derniers afin de déterminer l'incidence possible ou l'étendue des anomalies potentielles dans les états financiers, ou encore déterminer que l'entité a fourni des informations adéquates sur l'intrusion.
20. Par ailleurs, il est possible que les textes législatifs et réglementaires pouvant avoir une incidence directe ou indirecte sur les états financiers de l'entité comprennent des dispositions visant la protection des données. Lorsqu'il prend en considération la conformité de l'entité à ces textes législatifs et réglementaires, conformément à la norme ISA 250 (révisée)⁷⁴, l'auditeur peut être amené à prendre connaissance des processus informatiques de l'entité et des contrôles généraux informatiques que celle-ci a mis en œuvre pour se conformer aux textes législatifs et réglementaires en question.
21. Les contrôles généraux informatiques sont des contrôles que l'entité met en œuvre pour répondre aux risques provenant du recours à l'informatique. Pour les identifier, l'auditeur se fonde donc sur la connaissance qu'il a acquise à l'égard des applications informatiques et des autres aspects de l'environnement informatique qu'il a identifiés ainsi que des risques provenant du recours à l'informatique qui sont applicables. Lorsque l'entité utilise les mêmes processus informatiques pour l'ensemble de son environnement informatique ou pour certaines de ses applications informatiques, il est possible que l'auditeur identifie des risques communs provenant du recours à l'informatique et des contrôles généraux informatiques communs.

⁷⁴ Norme ISA 250 (révisée)

22. En règle générale, il est probable que les contrôles généraux informatiques portant sur les applications informatiques et sur les bases de données seront plus nombreux à être identifiés que ceux portant sur d'autres aspects de l'environnement informatique, puisque les premiers sont plus étroitement liés au traitement et au stockage des informations dans le système d'information de l'entité. Pour identifier les contrôles généraux informatiques, l'auditeur peut tenir compte non seulement des contrôles afférents aux actions posées par les utilisateurs finaux, mais aussi de ceux afférents aux actions posées par le personnel du service informatique ou par des fournisseurs de services informatiques.
23. L'**Annexe 6** fournit de plus amples explications sur la nature des contrôles généraux informatiques qui sont couramment mis en œuvre pour différents aspects de l'environnement informatique ainsi que des exemples de contrôles généraux informatiques pour certains processus informatiques.

Annexe 6

(Voir par. 25 (c)(ii) et A173–A174)

Éléments à prendre en considération pour prendre connaissance des contrôles généraux informatiques

La présente annexe contient des exemples d'éléments que l'auditeur peut prendre en considération pour prendre connaissance des contrôles généraux informatiques.

1. Nature des contrôles généraux informatiques couramment mis en œuvre pour chaque aspect de l'environnement informatique

(a) Applications

Les contrôles généraux informatiques qui sont mis en œuvre au niveau de la couche « applications informatiques » sont fonction de la nature et de l'étendue de la fonctionnalité des applications et des chemins d'accès qu'elles permettent d'emprunter. Ainsi, il y aura généralement plus de contrôles pertinents pour des applications informatiques hautement intégrées comportant des options de sécurité complexes que pour une application informatique développée en interne qui ne sert que pour un petit nombre de soldes de comptes et dans laquelle l'accès s'effectue uniquement à partir des opérations.

(b) Base de données

Les contrôles généraux informatiques qui sont mis en œuvre au niveau de la couche « base de données » visent généralement à répondre aux risques provenant du recours à l'informatique qui concernent les mises à jour non autorisées des informations financières contenues dans la base de données au moyen d'un accès direct à celle-ci ou de l'exécution d'un script ou d'un programme.

(c) Système d'exploitation

Les contrôles généraux informatiques qui sont mis en œuvre au niveau de la couche « système d'exploitation » visent généralement à répondre aux risques provenant du recours à l'informatique qui concernent les droits d'administrateur – droits qui peuvent faciliter le contournement d'autres contrôles. L'usurpation de l'authentifiant d'autres utilisateurs, l'ajout de nouveaux utilisateurs non autorisés, le téléchargement de logiciels malveillants et l'exécution de scripts ou d'autres programmes non autorisés en sont quelques exemples.

(d) Réseau

Les contrôles généraux informatiques qui sont mis en œuvre au niveau de la couche « réseau » visent généralement à répondre aux risques provenant du recours à l'informatique qui concernent la segmentation du réseau, l'accès à distance et l'authentification. Les contrôles du réseau peuvent être pertinents lorsque l'entité utilise des applications Web pour la présentation de l'information financière. Ces contrôles peuvent aussi être pertinents lorsque les relations avec les partenaires commerciaux ou les tiers fournisseurs de services occupent une place importante dans les activités de l'entité, car cela peut faire augmenter le volume de données transmises et nécessiter un accès à distance.

2. Exemples de contrôles généraux informatiques pouvant être mis en œuvre pour chaque type de processus informatique

(a) Processus de gestion des accès

- *Authentification*

Contrôles consistant à vérifier qu'un utilisateur accède à une application informatique ou à un autre élément de l'environnement informatique au moyen de son propre authentifiant (c'est-à-dire que celui-ci n'utilise pas l'authentifiant d'un autre utilisateur).

- *Autorisation*
Contrôles qui font que les utilisateurs ont uniquement accès aux informations dont ils ont besoin pour s'acquitter des responsabilités rattachées à leur poste, ce qui favorise une séparation des tâches appropriée.
 - *Attribution*
Contrôles attribuant des droits d'accès aux nouveaux utilisateurs et autorisant la modification des privilèges d'accès des utilisateurs existants.
 - *Révocation*
Contrôles révoquant les droits d'accès d'un utilisateur en cas de cessation d'emploi ou de mutation.
 - *Accès privilégié*
Contrôles afférents aux droits d'administrateur ou aux droits des utilisateurs avec pouvoir.
 - *Examen des accès utilisateurs*
Contrôles visant à évaluer ou à attester à nouveau l'autorisation continue des accès utilisateurs.
 - *Paramètres de sécurité*
Contrôles dont est généralement dotée chaque technologie consistant en des paramètres de configuration clés permettant de restreindre l'accès à l'environnement informatique.
 - *Accès physique*
Contrôles afférents à l'accès physique au centre de données et au matériel informatique afin d'éviter que cet accès puisse servir au contournement d'autres contrôles.
- (b) Processus de gestion des changements touchant les programmes ou d'autres changements apportés à l'environnement informatique
- *Processus de gestion des changements*
Contrôles afférents au processus visant la conception, la programmation et la mise à l'essai de changements ainsi qu'à leur intégration à l'environnement de production (utilisateur final).
 - *Séparation des tâches dans le cadre de l'intégration des changements à l'environnement de production*
Contrôles visant la séparation des droits d'accès aux fins de l'apport de changements et de leur intégration à l'environnement de production.
 - *Élaboration, acquisition ou mise en œuvre des systèmes*
Contrôles afférents à l'élaboration ou à la mise en œuvre initiale des applications informatiques (ou en lien avec d'autres aspects de l'environnement informatique).
 - *Conversion des données*
Contrôles afférents à la conversion des données durant l'élaboration, la mise en œuvre ou les mises à niveau de l'environnement informatique.

(c) Processus de gestion des opérations informatiques

- *Planification des travaux*
Contrôles afférents à l'accès permettant de planifier et de lancer des travaux ou des programmes pouvant avoir une incidence sur l'information financière.
- *Suivi des travaux*
Contrôles mis en œuvre pour assurer le suivi des travaux ou des programmes portant sur l'information financière en vue de leur bon déroulement.
- *Sauvegarde et récupération*
Contrôles mis en œuvre pour s'assurer que des sauvegardes des données liées à l'information financière ont lieu comme prévu et que ces données sont disponibles et rapidement récupérables en cas de panne ou d'attaque.
- *Détection des intrusions*
Contrôles mis en œuvre pour assurer la surveillance des points vulnérables de l'environnement informatique ou le suivi des intrusions dont il fait l'objet.

Des exemples de risques provenant du recours à l'informatique et des exemples de contrôles généraux informatiques qui peuvent être mis en œuvre pour y répondre, selon la nature de l'application informatique concernée, sont présentés dans le tableau ci-après.

Processus	Risques	Contrôles	Applications informatiques		
			Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
Gestion des accès	Privilèges d'accès : Utilisateurs détenant des privilèges d'accès supérieurs à ceux qui sont nécessaires pour l'exercice de leurs fonctions, ce qui peut compromettre la séparation des tâches.	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	Oui, au lieu de l'examen des accès utilisateurs mentionné ci-après	Oui	Oui

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
		donnant lieu à des informations financières critiques et la séparation des tâches.			
		Les droits d'accès sont rapidement révoqués ou modifiés en cas de cessation d'emploi ou de mutation de l'utilisateur.	Oui, au lieu de l'examen des accès utilisateurs mentionnés ci-après	Oui	Oui
		Les accès utilisateurs font l'objet d'un examen périodique.	Oui, au lieu des contrôles axés sur l'attribution et la révocation des droits d'accès décrits ci-dessus	Oui, pour certaines applications	Oui
		La séparation des tâches fait l'objet d'un suivi et les droits d'accès incompatibles sont soit abolis, soit mis en correspondance avec des contrôles d'atténuation des risques consignés par écrit et testés.	N/A, le système n'est pas doté de fonctionnalités visant à assurer la séparation des tâches	Oui, pour certaines applications	Oui
		Les privilèges d'accès (par	Oui, mais probablement	Oui, au niveau de la couche	Oui, à toutes les couches

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
		exemple, les droits d'administrateurs permettant de gérer la configuration, les données et la sécurité) sont strictement attribués aux utilisateurs autorisés.	seulement au niveau de la couche « applications informatiques »	« applications informatiques » et de certaines couches « environnement informatique » de la plateforme	« environnement informatique » de la plateforme
Gestion des accès	Accès direct aux données : Possibilité de modifier les données financières de façon inappropriée sans qu'une opération soit enregistrée dans une application.	L'accès aux fichiers de données des applications ou aux objets, tables ou données des bases de données est limité aux utilisateurs autorisés, en fonction des responsabilités et du rôle qui leur incombent, et cet accès est approuvé par la direction.	N/A	Oui, pour certaines applications et bases de données	Oui
Gestion des accès	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	Pour accéder aux systèmes, les utilisateurs doivent s'authentifier au moyen de codes d'utilisateur et de mots de passe uniques ou	Oui, authentification par mot de passe uniquement	Oui, authentification par mot de passe et authentification multifactorielle	Oui

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
	appropriés et dûment autorisés.	<p>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.).</p>			
	Applications : Modification inappropriée des systèmes/programmes d'application dotés de contrôles automatisés pertinents (paramètres configurables, algorithmes/calculs automatisés, extraction automatisée	Les modifications apportées aux applications sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.	N/A, si l'on s'est assuré qu'aucun code source n'est accessible	Oui, s'il s'agit de logiciels non commerciaux	Oui
		Les attributs clés des paramètres de sécurité sont mis en œuvre de façon appropriée.	N/A, aucun paramètre de sécurité	Oui, pour certaines applications et bases de données	Oui

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
	des données, etc.) ou de fonctionnalités logiques permettant de générer des rapports.	La possibilité d'intégrer des changements à l'environnement de production des applications est rigoureusement restreinte et il y a séparation des tâches par rapport à l'environnement de développement.	N/A	Oui, s'il s'agit de logiciels non commerciaux	Oui
Gestion des changements	Bases de données : Modification inappropriée de la structure des bases de données et des corrélations entre les données.	Les modifications apportées aux bases de données sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.	N/A, aucune modification apportée aux bases de données au sein de l'entité	Oui, s'il s'agit de logiciels non commerciaux	Oui
Gestion des changements	Logiciels de base : Modification inappropriée des logiciels de base (par exemple, système d'exploitation, réseau, logiciel de gestion des changements, logiciel de contrôle d'accès).	Les modifications apportées aux logiciels de base sont rigoureusement testées et approuvées avant d'être intégrées à l'environnement de production.	N/A, aucune modification apportée aux logiciels de base au sein de l'entité	Oui	Oui

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
Gestion des changements	Conversion des données : Introduction d'erreurs dans les données converties à partir de systèmes patrimoniaux ou de versions précédentes en raison de la présence de données incomplètes, redondantes, obsolètes ou inexactes dans ces systèmes ou versions.	La direction approuve les résultats de la conversion des données (après avoir rapproché et équilibré les comptes, par exemple) de l'ancien logiciel d'application ou de l'ancienne structure de données au nouveau logiciel d'application ou à la nouvelle structure de données et s'assure que la conversion a été effectuée conformément aux politiques et procédures de conversion établies.	N/A, recours à des contrôles manuels	Oui	Oui
Gestion des opérations informatiques	Réseau : Possibilité que des utilisateurs non autorisés accèdent aux systèmes d'information.	Pour accéder au réseau, 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.	N/A, l'accès au réseau n'est protégé par aucun mécanisme d'authentification distinct	Oui	Oui

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
		<p>Les paramètres des mots de passe répondent aux normes et aux politiques de l'entreprise ou de la profession (longueur minimale et niveau de complexité exigés, expiration du mot de passe, verrouillage du compte, etc.).</p>			
		<p>Le réseau est segmenté de manière à isoler les applications Web du réseau interne, où s'effectue l'accès aux applications soumises au contrôle interne à l'égard de l'information financière.</p>	<p>N/A, réseau non segmenté</p>	<p>Oui, en faisant preuve de jugement</p>	<p>Oui, en faisant preuve de jugement</p>
		<p>Les gestionnaires du réseau effectuent périodiquement des analyses de vulnérabilité du périmètre du réseau et procèdent à des investigations</p>	<p>N/A</p>	<p>Oui, en faisant preuve de jugement</p>	<p>Oui, en faisant preuve de jugement</p>

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
		quant aux vulnérabilités potentielles.			
		Des alertes sont générées périodiquement pour signaler les menaces relevées par les systèmes de détection des intrusions. Les gestionnaires du réseau procèdent à des investigations au sujet de ces menaces.	N/A	Oui, en faisant preuve de jugement	Oui, en faisant preuve de jugement
		Des contrôles sont en place pour restreindre l'accès au réseau privé virtuel (« VPN ») aux seuls utilisateurs autorisés et appropriés.	N/A, pas de « VPN »	Oui, en faisant preuve de jugement	Oui, en faisant preuve de jugement
Gestion des opérations informatiques	Sauvegarde et récupération des données : Impossibilité de récupérer ou de consulter rapidement les données financières en cas de perte de données.	Les données financières sont sauvegardées régulièrement selon un calendrier et une fréquence établis.	N/A, les données doivent être récupérées manuellement par l'équipe des finances.	Oui	Oui

Processus	Risques	Contrôles	Applications informatiques		
Processus informatique	Exemples de risques provenant du recours à l'informatique	Exemples de contrôles généraux informatiques	Applicables aux logiciels commerciaux peu complexes ?	Applicables aux logiciels commerciaux ou aux applications informatiques de moyenne envergure et modérément complexes ?	Applicables aux applications informatiques de grande envergure ou complexes (par exemple, progiciels de gestion intégrés) ?
Gestion des opérations informatiques	Planification des travaux : Traitement inexact, incomplet ou non autorisé des données dans les systèmes, programmes ou travaux de production.	Seuls les utilisateurs autorisés peuvent effectuer la mise à jour des travaux par lots (avec ou sans interface) dans le logiciel de planification des travaux.	N/A, aucun travail par lots	Oui, pour certaines applications	Oui
		Les systèmes, programmes et travaux essentiels font l'objet d'un suivi et les erreurs de traitement sont corrigées afin d'assurer l'intégrité du traitement.	N/A, aucun suivi des travaux	Oui, pour certaines applications	Oui

MODIFICATIONS DE CONCORDANCE ET MODIFICATIONS CORRÉLATIVES APPORTÉES À D'AUTRES NORMES INTERNATIONALES

À noter : Les modifications de concordance présentées ici sont apportées à d'autres normes internationales conséquemment à l'approbation de la norme ISA 315 (révisée en 2019). Elles entreront en vigueur en même temps que la norme ISA 315 (révisée en 2019). Les changements apportés par rapport aux dernières versions approuvées des normes internationales sont indiqués en suivi des modifications. La numérotation des notes de bas de page ci-dessous ne correspond pas à celle employée dans les normes internationales faisant l'objet des modifications ; il convient donc de se reporter à ces normes. Le Conseil de supervision de l'intérêt public (PIOB) a approuvé les présentes modifications de concordance. Il a en effet conclu que ces modifications ont été élaborées dans le respect de la procédure officielle et que l'intérêt public a dûment été pris en compte.

Norme ISA 200, *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux normes internationales d'audit*

Champ d'application de la présente norme ISA

[...]

L'audit d'états financiers

[...]

7. Les normes ISA contiennent des objectifs, des diligences ainsi que des modalités d'application et autres commentaires explicatifs qui sont conçus pour aider l'auditeur à obtenir une assurance raisonnable. Elles requièrent de l'auditeur qu'il exerce son jugement professionnel et fasse preuve d'esprit critique tout au long de la planification et de la réalisation de l'audit et, entre autres :
 - qu'il identifie et évalue les risques d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs, en se fondant sur sa connaissance de l'entité et de son environnement, ~~y compris son~~ du référentiel comptable applicable et du système de contrôle interne de l'entité ;
 - qu'il recueille, en concevant et en mettant en œuvre des réponses adaptées à l'évaluation des risques, des éléments probants suffisants et appropriés indiquant s'il existe des anomalies significatives ;
 - qu'il se forme une opinion sur les états financiers à partir des conclusions tirées des éléments probants recueillis.

[...]

Date d'entrée en vigueur

[...]

Objectifs généraux de l'auditeur

[...]

Définitions

13. Dans les normes ISA, on entend par :

[...]

- (n) « risque d'anomalies significatives », le risque que les états financiers comportent des anomalies significatives avant l'audit. Ce risque comprend deux composantes, définies comme suit au niveau des assertions : (Voir par. A15a)
 - (i) « risque inhérent », la possibilité qu'une assertion portant sur un flux d'opérations, un solde de compte ou une information à fournir comporte une anomalie qui pourrait être significative, individuellement ou cumulée avec d'autres, avant prise en considération des contrôles y afférents,
 - (ii) « risque lié au contrôle interne », le risque qu'une anomalie qui pourrait se produire au niveau d'une assertion portant sur un flux d'opérations, un solde de compte ou une information à fournir et qui pourrait être significative, individuellement ou cumulée avec d'autres, ne soit ni prévenue ni détectée et corrigée en temps ~~venu~~ opportun par les ~~contrôles interne~~ de l'entité ;

Diligences

Règles de déontologie relatives à un audit d'états financiers

[...]

Esprit critique

[...]

Jugement professionnel

[...]

Éléments probants suffisants et appropriés et risque d'audit

17. Pour obtenir une assurance raisonnable, l'auditeur doit recueillir des éléments probants suffisants et appropriés pour ramener le risque d'audit à un niveau suffisamment faible et être ainsi en mesure de tirer des conclusions raisonnables sur lesquelles fonder son opinion. (Voir par. A30–A54)

Réalisation d'un audit conforme aux normes ISA

Respect des normes ISA pertinentes pour l'audit

[...]

19. L'auditeur doit avoir acquis une connaissance de l'intégralité du texte d'une norme ISA, y compris ses modalités d'application et autres commentaires explicatifs, pour en comprendre les objectifs et en appliquer correctement les diligences. (Voir par. A60–A68)

[...]

Objectifs particuliers des différentes normes ISA

[...]

Conformité aux diligences pertinentes

[...]

Incapacité d'atteindre un objectif

[...]

Modalités d'application et autres commentaires explicatifs

L'audit d'états financiers

Étendue de l'audit (Voir par. 3)

[...]

Préparation des états financiers (Voir par. 4)

[...]

Considérations propres aux audits dans le secteur public

[...]

Forme de l'opinion de l'auditeur (Voir par. 8)

[...]

Définitions

États financiers (Voir par. 13 (f))

[...]

Risque d'anomalies significatives (Voir par. 13 (n))

A15a. Pour les besoins des normes ISA, on considère qu'il existe un risque d'anomalies significatives lorsqu'il y a une possibilité raisonnable qu'une anomalie :

- (a) se produise (critère de probabilité) :

- (b) soit significative si elle se produit (critère d'ampleur).

Règles de déontologie relatives à un audit d'états financiers (Voir par. 14)

[...]

Esprit critique (Voir par. 15)

[...]

Jugement professionnel (Voir par. 16)

Éléments probants suffisants et appropriés et risque d'audit (Voir par. 5 et 17)

Caractère suffisant et approprié des éléments probants

A30. Les éléments probants sont nécessaires pour étayer l'opinion et le rapport de l'auditeur. Ils sont cumulatifs par nature et sont principalement recueillis au moyen des procédures d'audit réalisées lors de l'audit. Cependant, ils peuvent également comprendre des informations obtenues d'autres sources telles que les audits antérieurs (sous réserve que l'auditeur ait déterminé s'il est survenu depuis des changements susceptibles d'affecter la pertinence de ces informations pour l'audit en cours⁷⁵) ou les procédures de contrôle qualité appliquées par le cabinet pour l'acceptation ou le maintien d'une relation client. Les documents comptables de l'entité constituent une source importante d'éléments probants, parallèlement à d'autres sources internes ou externes à l'entité. Par ailleurs, certaines informations utilisables en tant qu'éléments probants peuvent avoir été produites par un employé expert ou un tiers expert dont l'entité a retenu les services. Les éléments probants comprennent à la fois les informations qui étayent et corroborent les assertions de la direction et les informations qui les contredisent. De plus, dans certains cas, l'absence d'informations (par exemple, le refus de la direction de fournir une déclaration requise) est prise en compte par l'auditeur, et constitue par conséquent un élément probant. La plupart des travaux qu'effectue l'auditeur en vue de se former une opinion consistent à recueillir et à évaluer des éléments probants.

[...]

Risque d'audit

[...]

Risques d'anomalies significatives

[...]

A40. Le risque inhérent varie selon les facteurs de risque inhérent, est plus élevé pour certaines assertions et pour les flux d'opérations, soldes de comptes ou informations à fournir qui s'y rapportent que pour d'autres. Le degré de risque inhérent dépend de la mesure dans laquelle les facteurs de risque inhérent influent sur la possibilité qu'une assertion comporte des anomalies, et s'inscrit sur une échelle appelée « échelle de risque inhérent ». L'auditeur détermine les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes, ainsi que les assertions

⁷⁵ Norme ISA 315 (révisée en 2019), *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives*, paragraphe 916.

pertinentes les concernant, au cours du processus d'identification et d'évaluation des risques d'anomalies significatives. Par exemple, il peut être plus élevé dans le cas de calculs complexes ou de il se peut que des soldes de comptes comportant des montants provenant d'estimations comptables qui présentent une incertitude d'estimation importante soient identifiés comme étant des soldes de comptes importants et qu'en raison de cette incertitude, l'évaluation du risque inhérent que fait l'auditeur pour les risques au niveau des assertions se rattachant à ces soldes de comptes se situe à un niveau supérieur.

A40a. Des facteurs externes à l'origine de certains risques liés à l'activité peuvent également influencer sur le risque inhérent. Par exemple, l'évolution technologique peut rendre obsolète un produit donné, et augmenter de ce fait le risque d'une surévaluation des stocks. Des facteurs caractérisant l'entité et son environnement et concernant l'ensemble ou une partie des flux d'opérations, soldes de comptes ou informations à fournir peuvent également influencer sur le risque inhérent lié à une assertion particulière. Un fonds de roulement insuffisant pour poursuivre les activités ou un secteur d'activité en déclin caractérisé par un grand nombre de faillites constituent des exemples possibles de tels facteurs.

A41. Le risque lié au contrôle interne est fonction de l'efficacité de la conception, de la mise en œuvre et du maintien par la direction des contrôles internes nécessaires pour faire face aux risques identifiés pouvant compromettre l'atteinte des objectifs de l'entité concernant la préparation des états financiers. Toutefois, le contrôle interne, quelle que soit la qualité de sa conception et de son fonctionnement, peut seulement réduire et non pas éliminer les risques d'anomalies significatives dans les états financiers, et ce, en raison des limites qui lui sont inhérentes aux contrôles. Celles-ci comprennent par exemple la possibilité d'erreurs ou de fautes humaines ou encore de neutralisation des contrôles, que ce soit en raison de collusions ou de leur contournement par la direction. En conséquence, il subsistera toujours un certain risque lié au contrôle interne. Les normes ISA précisent dans quelles situations l'auditeur est tenu, ou peut choisir, de tester l'efficacité du fonctionnement des contrôles pour déterminer la nature, le calendrier et l'étendue des contrôles de substance à mettre en œuvre⁷⁶.

A42.⁷⁷ L'évaluation des risques d'anomalies significatives peut s'exprimer en termes quantitatifs, par exemple en pourcentages, ou en termes non quantitatifs. Quoi qu'il en soit, c'est le caractère approprié des évaluations des risques faites par l'auditeur qui compte, plus que le choix de la démarche adoptée. En général, dans les normes ISA, on parle de « risques d'anomalies significatives » ; on ne traite pas séparément du risque inhérent et du risque lié au contrôle interne, mais parlent plutôt d'une évaluation globale des « risques d'anomalies significatives ». Cela dit, Toutefois, la norme ISA 540315 (révisée en 2019)⁷⁸ requiert une évaluation séparée du que l'auditeur évalue séparément le risque inhérent et du le risque lié au contrôle interne afin d'établir un fondement de disposer d'une base pour la conception et la mise en œuvre des procédures d'audit complémentaires en réponse aux risques d'anomalies significatives, y compris les risques importants, au niveau des assertions liés aux estimations comptables, conformément à la norme

⁷⁶ Norme ISA 330, *Réponses de l'auditeur à l'évaluation des risques*, paragraphes 7–17.

⁷⁷ Remarque : Dans le paragraphe A42 de la norme ISA 200, les changements sont indiqués par rapport au paragraphe ayant auparavant fait l'objet de modifications de concordance dans le cadre de la révision de la norme ISA 540 (révisée).

⁷⁸ Norme ISA 540315 (révisée en 2019), *Audit des estimations comptables et des informations y afférentes*, paragraphe 15 *Identification et évaluation des risques d'anomalies significatives*.

~~ISA 330⁷⁹. Pour l'identification et l'évaluation des risques d'anomalies significatives liés aux flux d'opérations importantes, aux soldes de comptes importants ou aux informations à fournir importantes qui ne se rapportent pas aux estimations comptables, l'auditeur peut procéder à une évaluation séparée ou globale du risque inhérent et du risque lié au contrôle en fonction des techniques ou des méthodes d'audit privilégiées ainsi que de considérations pratiques.~~

A43a. L'évaluation des risques d'anomalies significatives au niveau des assertions vise à permettre de déterminer la nature, le calendrier et l'étendue des procédures d'audit complémentaires nécessaires pour recueillir des éléments probants suffisants et appropriés⁸⁰.

Risque de non-détection

[...]

Limites inhérentes à l'audit

[...]

Nature de l'information financière

[...]

Nature des procédures d'audit

[...]

Célérité et rapport coût-avantage en matière d'information financière

[...]

A52. Compte tenu des approches décrites au paragraphe A51, les normes ISA contiennent des diligences concernant la planification et la réalisation de l'audit, et imposent entre autres à l'auditeur :

- de mettre en œuvre des procédures d'évaluation des risques et des procédures liées afin de disposer d'une base pour l'identification et l'évaluation des risques d'anomalies significatives ~~aux niveaux des états financiers et~~ au niveau des assertions⁸¹ ;
- de recourir à des tests et à d'autres méthodes d'étude de populations afin de disposer d'une base raisonnable pour tirer des conclusions sur la population étudiée⁸².

Autres facteurs influant sur les limites inhérentes à l'audit

[...]

Réalisation d'un audit conforme aux normes ISA

Nature des normes ISA (Voir par. 18)

[...]

⁷⁹ Norme ISA 330, par. 7 b).

⁸⁰ Norme ISA 330, paragraphe 6.

⁸¹ Norme ISA 315 (révisée en 2019), paragraphes 517 à 4022.

⁸² Norme ISA 330, norme ISA 500, norme ISA 520, *Procédures analytiques*, et norme ISA 530, *Sondages en audit*.

Considérations propres aux audits dans le secteur public

[...]

Contenu des normes ISA (Voir par. 19)

A60. Outre des objectifs et des diligences (les diligences étant signalées dans les normes ISA par l'emploi du verbe « devoir »), une norme ISA contient des indications connexes sous la forme de modalités d'application et autres commentaires explicatifs. Elle peut également comporter des paragraphes d'introduction lorsqu'une mise en contexte est utile à une bonne connaissance de la norme, ainsi que des définitions. L'intégralité du texte d'une norme ISA est donc pertinente pour la connaissance des objectifs particuliers de la norme et une bonne application de ses diligences.

A61. Les « modalités d'application et autres commentaires explicatifs » fournissent un complément d'explications sur les diligences de la norme ainsi que des indications de mise en œuvre. Il se peut notamment que ces dispositions comportent :

- des précisions sur le sens ou la portée d'une exigence, y compris, dans certaines normes ISA telles que la norme ISA 315 (révisée en 2019), les raisons pour lesquelles une procédure est exigée ;
- des exemples de procédures pouvant être appropriées dans les circonstances. Dans certaines normes ISA telles que la norme ISA 315 (révisée en 2019), les exemples sont présentés dans des encadrés.

Même si de telles indications n'imposent pas en soi de diligences, elles sont utiles à une bonne application des diligences de la norme. Les « modalités d'application et autres commentaires explicatifs » peuvent également contenir des informations générales sur certains points dont traite la norme.

[...]

Considérations ~~propres aux petites entités~~ relatives à l'application proportionnée

A65a. Des considérations relatives à l'application proportionnée ont été incluses dans certaines normes ISA, par exemple la norme ISA 315 (révisée en 2019), afin d'illustrer l'application des diligences à toutes les entités, que leur nature et leurs circonstances soient peu complexes ou non. Les entités peu complexes présentent généralement les caractéristiques énumérées au paragraphe A66.

A65b. Les « considérations propres aux petites entités » que contiennent ~~les certaines~~ normes ISA ont été élaborées avant tout dans la perspective d'entités non cotées. Toutefois, certaines de ces considérations peuvent être utiles pour l'audit de petites entités cotées.

A66. Aux fins des considérations supplémentaires propres à l'audit de petites entités, le terme « petite entité » s'entend d'une entité qui possède généralement les caractéristiques qualitatives suivantes :

- (a) concentration de la propriété et de la direction entre les mains d'un petit nombre de personnes (souvent une personne unique : soit une personne physique, soit une autre entreprise propriétaire de l'entité, à condition que son propriétaire présente les caractéristiques qualitatives pertinentes) ;

- (b) une ou plusieurs des particularités suivantes :
- (i) des opérations classiques ou dénuées de complexité,
 - (ii) une comptabilité simple,
 - (iii) un nombre restreint de branches d'activité et de produits par branche d'activité,
 - (iv) ~~peu~~ un système de contrôles internes simple,
 - (v) un nombre restreint d'échelons de direction, ayant toutefois la responsabilité d'un large éventail de contrôles,
 - (vi) des effectifs limités, dont beaucoup ont un large éventail de tâches.

Ces caractéristiques qualitatives ne constituent pas une liste exhaustive, elles ne sont pas l'apanage des petites entités et les petites entités ne les présentent pas nécessairement toutes.

A67. *[Devenu le paragraphe A65b]*

Considérations relatives aux outils et aux techniques automatisés

A67a. Les « considérations relatives aux outils et aux techniques automatisés » que contiennent certaines normes ISA, par exemple la norme ISA 315 (révisée en 2019), ont été élaborées pour expliquer comment l'auditeur peut appliquer certaines diligences lorsqu'il a recours à des outils et à des techniques automatisés pour mettre en œuvre des procédures d'audit.

Objectifs particuliers des différentes normes ISA (Voir par. 21)

[...]

Détermination, au moyen des objectifs, de la nécessité de mettre en œuvre des procédures d'audit supplémentaires (Voir par. 21 (a))

[...]

Évaluation, au regard des objectifs, du caractère suffisant et approprié des éléments probants recueillis (Voir par. 21 (b))

[...]

Respect des diligences pertinentes

Diligences pertinentes (Voir par. 22)

[...]

Dérogation à une exigence (Voir par. 23)

[...]

Incapacité d'atteindre un objectif (Voir par. 24)

[...]

Norme ISA 210, *Accord sur les termes et conditions d'une mission d'audit*

Modalités d'application et autres commentaires explicatifs

[...]

Conditions préalables à la réalisation d'une mission d'audit

[...]

Accord sur les responsabilités de la direction (Voir par. 6 (b))

[...]

Contrôle interne (Voir sous-paragraphe 6 (b)(ii))

[...]

A18. Il appartient à la direction de déterminer quel contrôle interne est nécessaire pour la préparation des états financiers. La notion de contrôle interne englobe une large gamme de mesures dans le cadre de composantes du système de contrôle interne que l'on peut désigner sous les noms suivants : environnement de contrôle ; processus d'évaluation des risques par l'entité ; processus de suivi du système de contrôle interne par l'entité ; système d'information (~~y compris les processus opérationnels connexes~~) pertinent pour l'information financière, et communications ; et mesures de contrôle ; ~~et suivi des contrôles~~. Cependant, cette décomposition du contrôle interne ne reflète pas nécessairement la manière dont une entité en particulier conçoit, met en œuvre et maintient son propre contrôle interne, ni la façon dont elle peut en classer les différentes composantes⁸³. Le contrôle interne d'une entité (en particulier ses livres et documents comptables ou ses systèmes comptables) est le reflet des besoins de la direction, de la complexité des activités de l'entité, de la nature des risques auxquels elle est exposée et des textes légaux ou réglementaires pertinents.

Norme ISA 230, *Documentation de l'audit*

Modalités d'application et autres commentaires explicatifs

[...]

Documentation des procédures d'audit réalisées et des éléments probants recueillis

[...]

Identification des éléments spécifiques testés, et des personnes responsables de l'exécution et de la revue des travaux (Voir par. 9)

[...]

Considérations propres aux petites entités (Voir par. 8)

[...]

⁸³ Norme ISA 315 (révisée en 2019), paragraphe A9159 et Annexe 34.

A17. Lors de la préparation de la documentation de l'audit, l'auditeur d'une petite entité peut juger utile et efficient de consigner des informations concernant différents aspects de l'audit dans un même document avec, au besoin, des références à des feuilles de travail complémentaires. Voici des exemples de points pouvant être documentés ensemble lors de l'audit d'une petite entité : connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité; stratégie générale d'audit et programme de travail; seuils de signification déterminés conformément à la norme ISA 320⁸⁴; évaluation des risques; questions importantes notées au cours de l'audit et conclusions tirées.

[...]

Norme ISA 250 (révisée), *Prise en compte des textes légaux et réglementaires dans un audit d'états financiers*

Modalités d'application et autres commentaires explicatifs

[...]

Procédures d'audit à mettre en œuvre lorsqu'un cas de non-conformité est identifié ou suspecté

[...]

Appréciation des conséquences des cas identifiés ou suspectés de non-conformité (Voir par. 22)

A23. Comme il est exigé au paragraphe 22, l'auditeur apprécie les conséquences des cas identifiés ou suspectés de non-conformité aux textes légaux ou réglementaires sur d'autres aspects de l'audit, notamment son évaluation des risques et la fiabilité des déclarations écrites. Les conséquences de cas particuliers identifiés ou suspectés de non-conformité dépendront du lien entre la perpétration de l'acte et sa dissimulation, le cas échéant, et des ~~activités spécifiques de contrôles spécifiques~~ de l'entité, ainsi que du niveau de la direction ou des personnes travaillant pour l'entité impliquée ou sous sa direction, tout particulièrement les conséquences découlant de l'implication du niveau d'autorité le plus élevé dans l'entité. Comme il est indiqué au paragraphe 9, la conformité de l'auditeur aux textes légaux ou réglementaires ou aux règles de déontologie pertinentes peut fournir des informations supplémentaires qui sont utiles aux fins de l'accomplissement de ses responsabilités conformément au paragraphe 22.

[...]

Norme ISA 260 (révisée), *Communication avec les personnes constituant le gouvernement d'entreprise*

Modalités d'application et autres commentaires explicatifs

[...]

⁸⁴ Norme ISA 320, *Caractère significatif dans la planification et la réalisation d'un audit.*

Questions à communiquer

[...]

Étendue et calendrier prévus des travaux d'audit (Voir par. 15)

[...]

A12. Le fait de communiquer les risques importants identifiés par l'auditeur aide les personnes constituant le gouvernement d'entreprise à comprendre ces points et les raisons pour lesquelles ils ont été identifiés comme des risques importants ~~exigent une attention spéciale sur le plan de l'audit~~. La communication des risques importants peut aussi aider les personnes constituant le gouvernement d'entreprise à s'acquitter de leur responsabilité de surveillance du processus d'information financière.

A13. Les questions communiquées peuvent notamment porter sur :

- la façon dont l'auditeur prévoit de répondre aux risques importants d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs ;
- la façon dont l'auditeur prévoit de tenir compte des aspects qui, selon son évaluation, comportent les risques d'anomalies significatives les plus élevés ;
- la démarche de l'auditeur concernant ~~les aspects du~~ le système de contrôle interne de l'entité pertinents pour l'audit ;
- l'application du concept de caractère significatif dans le contexte d'un audit ;
- [...]

Annexe 2

(Voir par. 16 (a) et par. A19–A20)

Aspects qualitatifs des pratiques comptables

La communication requise par le paragraphe 16 (a), et commentée aux paragraphes A19–A20, peut porter notamment sur les questions qui suivent :

[...]

Estimations comptables

Pour les éléments donnant lieu à des estimations importantes, les questions traitées dans la norme ISA 540 (révisée)¹, y compris, par exemple :

- la manière dont la direction identifie les opérations, événements ~~et~~ ou conditions pouvant nécessiter la comptabilisation ou la présentation d'estimations comptables dans les états financiers ;

[...]

Norme ISA 265, Communication des déficiences dans le contrôle interne aux personnes constituant le gouvernement d'entreprise et à la direction

Introduction

Champ d'application de la présente norme ISA

1. La présente norme internationale d'audit (ISA) traite de la responsabilité qui incombe à l'auditeur de communiquer de façon appropriée aux personnes constituant le gouvernement d'entreprise et à la direction les déficiences dans le contrôle interne¹ qu'il a relevées au cours d'un audit d'états financiers. La présente norme ISA n'impose pas à l'auditeur d'autres responsabilités que celles dont traitent la norme ISA 315 (révisée en 2019) et la norme ISA 330² en ce qui concerne la prise de connaissance du système de contrôle interne de l'entité ainsi que la conception et la mise en œuvre de tests de procédures. Par ailleurs, la norme ISA 260 (révisée)³ définit des diligences additionnelles et fournit des indications au sujet de la responsabilité qu'a l'auditeur de communiquer avec les personnes constituant le gouvernement d'entreprise dans le cadre de l'audit.
2. L'auditeur est tenu de prendre connaissance ~~des aspects~~ du système de contrôle interne de l'entité pertinents pour l'audit lorsqu'il identifie et évalue les risques d'anomalies significatives⁴. Dans l'évaluation de ces risques, l'auditeur prend en considération le système de contrôle interne de l'entité afin de concevoir des procédures d'audit appropriées aux circonstances, et non dans le but d'exprimer une opinion sur l'efficacité du contrôle interne de l'entité. L'auditeur peut relever des déficiences de contrôle dans le contrôle interne au cours du processus d'évaluation de ces risques, mais aussi à d'autres stades de l'audit. La présente norme ISA précise quelles sont, parmi les déficiences relevées, celles que l'auditeur est tenu de communiquer aux personnes constituant le gouvernement d'entreprise et à la direction.

[...]

Modalités d'application et autres commentaires explicatifs

Déficiences dans le contrôle interne relevées ou non au cours de l'audit (Voir par. 7)

[...]

Considérations propres aux petites entités

- A3. Les contrôles ~~mesures de contrôle~~ de la composante « mesures de contrôle » reposent habituellement sur les mêmes concepts, quelle que soit la taille de l'entité, mais la mesure dans laquelle leur mode de fonctionnement est structuré le degré de formalité de leur mise en œuvre n'est pas toujours la même. En outre, de petites entités peuvent juger que certains types de contrôles ~~d'mesures de contrôle~~ ne sont pas nécessaires en raison des contrôles exercés par la direction. Par exemple, le fait de centraliser la centralisation auprès de la direction le du pouvoir d'autoriser l'octroi de crédit aux clients et d'approuver les achats importants peut ~~constituer un tenir lieu de~~ constituer un tenir lieu de contrôle efficace à l'égard ~~d'sur certains des opérations et de soldes de comptes importants principaux et certaines des opérations principales,~~ d'opérations principales, réduisant ou éliminant ainsi la nécessité de contrôles ~~de~~ d'mesures de contrôle plus détaillées.

[...]

Déficiences importantes du contrôle interne (Voir par. 6 (b) et par. 8)

[...]

- A8. Un contrôle peut être conçu pour assurer soit individuellement, soit en association avec d'autres contrôles, la prévention, ou la détection et la correction, des anomalies⁵. Par exemple, les contrôles sur les créances peuvent être constitués tant de contrôles automatisés que de contrôles manuels, tous ces contrôles étant conçus pour fonctionner en association afin de prévenir, ou de détecter et corriger, les anomalies dans le solde de compte en question. Une déficience du contrôle interne n'est pas nécessairement à elle seule suffisamment grave pour constituer une déficience importante. Cependant, une combinaison de déficiences touchant un même solde de compte, une même information à fournir, une même assertion ~~pertinente~~ ou une même composante du système de contrôle interne de l'entité peut accroître les risques d'anomalies au point de constituer une déficience importante.

Norme ISA 240, Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers

Introduction

Champ d'application de la présente norme ISA

[...]

Caractéristiques de la fraude

[...]

Responsabilité à l'égard de la prévention et de la détection des fraudes

[...]

Responsabilités de l'auditeur

[...]

7. En outre, le risque pour l'auditeur de ne pas détecter une anomalie significative résultant d'une fraude commise par la direction est plus élevé qu'en cas de fraude commise par les employés, car les dirigeants sont fréquemment à même de manipuler directement ou indirectement les documents comptables, de présenter des informations financières mensongères ou de contourner les ~~procédures de contrôles~~ conçues pour prévenir la perpétration de fraudes semblables par les employés.

[...]

Date d'entrée en vigueur

[...]

Objectifs

[...]

Définitions

[...]

Diligences

Esprit critique

12. Conformément à la norme ISA 200⁸⁵, l'auditeur doit faire preuve d'esprit critique tout au long de la mission, en étant conscient de l'existence possible d'une anomalie significative résultant d'une fraude, nonobstant le jugement que son expérience passée auprès de l'entité l'a amené à porter sur l'honnêteté et l'intégrité de la direction et des personnes constituant le gouvernement d'entreprise. (Voir par. A7– A8)
13. À moins d'avoir des raisons de croire le contraire, l'auditeur peut tenir les livres et autres documents comptables pour authentiques. Si des situations rencontrées au cours de l'audit l'amènent à douter de l'authenticité d'un document ou à penser que le contenu d'un document a été modifié sans qu'il en ait été informé, il doit procéder à des investigations complémentaires. (Voir par. A9)
14. Lorsque les réponses de la direction ou des personnes constituant le gouvernement d'entreprise à ses demandes d'informations sont incohérentes, l'auditeur doit procéder à des investigations sur ces incohérences.

Entretiens entre les membres de l'équipe affectés à la mission

15. La norme ISA 315 (révisée en 2019) requiert que des entretiens aient lieu entre les membres de l'équipe affectée à la mission et que l'associé responsable de la mission détermine les points qui sont à communiquer aux membres de l'équipe n'ayant pas participé aux entretiens⁸⁶. Ces entretiens doivent viser tout particulièrement à déterminer où et comment les états financiers de l'entité sont susceptibles de comporter des anomalies significatives résultant de fraudes, et comment une fraude aurait pu être perpétrée. Les entretiens doivent se dérouler en faisant abstraction de la confiance que les membres de l'équipe peuvent avoir dans l'honnêteté et l'intégrité de la direction et des personnes constituant le gouvernement d'entreprise. (Voir par. A10–A11)

Procédures d'évaluation des risques et procédures liées

16. Lorsque l'auditeur met en œuvre des procédures d'évaluation des risques et procède à des procédures liées afin de prendre connaissance de l'entité et de son environnement, ~~y compris le du référentiel comptable applicable et du système de~~ contrôle interne de l'entité, comme l'exige la norme ISA 315 (révisée en 2019)⁸⁷, il doit mettre en œuvre les procédures énumérées aux paragraphes ~~4723–2443~~ pour obtenir des informations qui lui serviront à identifier les risques d'anomalies significatives résultant de fraudes.

⁸⁵ Norme ISA 200, paragraphe 15.

⁸⁶ Norme ISA 315 (révisée en 2019), paragraphes ~~4017~~ et 18.

⁸⁷ Norme ISA 315 (révisée), paragraphes 5–24.

Direction et autres personnes au sein de l'entité

[...]

Personnes constituant le gouvernement d'entreprise

20. À moins que tous les personnes constituant le gouvernement d'entreprise ne participent à la gestion de l'entité⁸⁸, l'auditeur doit prendre connaissance de la façon dont ils exercent leur surveillance sur les procédures mises en œuvre par la direction pour identifier les risques de fraude dans l'entité et pour y répondre, ainsi que sur les contrôles interne établis par la direction pour réduire ces risques. (Voir par. A19–A21)

[...]

Identification de corrélations inhabituelles ou inattendues

[...]

Autres informations

23. L'auditeur doit se demander si d'autres informations qu'il a obtenues indiquent des risques d'anomalies significatives résultant de fraudes. (Voir par. A22)

Évaluation des facteurs de risque de fraude

24. L'auditeur doit évaluer si les informations qu'il a obtenues lors de la mise en œuvre des autres procédures d'évaluation des risques et des procédures liées indiquent la présence d'un ou de plusieurs facteurs de risque de fraude. Bien que la présence de facteurs de risque de fraude n'indique pas nécessairement l'existence de fraudes, ces facteurs sont souvent présents dans les situations de fraude et peuvent donc indiquer des risques d'anomalies significatives résultant de fraudes. (Voir par. A23–A27)

Identification et évaluation des risques d'anomalies significatives résultant de fraudes

25. Conformément à la norme ISA 315 (révisée en 2019), l'auditeur doit identifier et évaluer les risques d'anomalies significatives résultant de fraudes au niveau des états financiers pris dans leur ensemble et au niveau des assertions pour les flux d'opérations, les soldes de comptes et les informations à fournir dans les états financiers⁸⁹.
26. Lors de l'identification et de l'évaluation des risques d'anomalies significatives résultant de fraudes, en se fondant sur la présomption qu'il existe des risques de fraude dans la comptabilisation des produits, l'auditeur doit évaluer quelles catégories de produits, d'opérations génératrices de produits ou d'assertions peuvent être à l'origine de tels risques. Le paragraphe 47 donne des précisions sur la documentation exigée de l'auditeur dans les cas où il conclut que la présomption ne s'applique pas dans le contexte de la mission et qu'il n'a donc pas identifié la comptabilisation des produits comme étant à l'origine d'un risque d'anomalies significatives résultant de fraudes. (Voir par. A28–A30)

⁸⁸ Norme ISA 260 (révisée), *Communication avec les responsables de la gouvernance*, paragraphe 13.

⁸⁹ Norme ISA 315 (révisée en 2019), paragraphe 2825.

27. L'auditeur doit considérer les risques d'anomalies significatives résultant de fraudes qu'il a identifiés comme des risques importants et, en conséquence, s'il ne l'a pas déjà fait, ~~prendre connaissance des identifier les contrôles correspondants de l'entité, y compris les mesures de contrôle, qui sont pertinents par rapport à~~ visant à répondre à ces risques, évaluer leur conception et déterminer s'ils ont été mis en œuvre⁹⁰. (Voir par. A31–A32)

Réponses à l'évaluation des risques d'anomalies significatives résultant de fraudes

Approche générale

[...]

Procédures d'audit en réponse à l'évaluation des risques d'anomalies significatives résultant de fraudes au niveau des assertions

[...]

Procédures d'audit en réponse aux risques de contournement des contrôles par la direction

[...]

32. Indépendamment de son évaluation des risques de contournement des contrôles par la direction, l'auditeur doit concevoir et mettre en œuvre des procédures d'audit destinées :

- (a) à vérifier le caractère approprié des écritures comptables enregistrées dans le grand livre et des autres ajustements effectués lors de l'établissement des états financiers. Lorsqu'il conçoit et met en œuvre des procédures d'audit en vue de cette vérification, l'auditeur doit :
 - (i) s'enquérir auprès des personnes participant au processus d'information financière de toute activité inappropriée ou inhabituelle concernant le traitement des écritures comptables et des autres ajustements,
 - (ii) sélectionner des écritures comptables et d'autres ajustements effectués à la fin de la période,
 - (iii) considérer la nécessité de procéder à des tests sur les écritures comptables et les autres ajustements comptables effectués tout au long de la période ; (Voir par. A41– A44)

[...]

Évaluation des éléments probants (Voir par. A49)

[...]

Impossibilité de poursuivre la mission

[...]

Déclarations écrites

[...]

⁹⁰ Norme ISA 315 (révisée en 2019), sous-par. 26 (a)(i) et par. 26 (d).

Communication avec la direction et avec les personnes constituant le gouvernement d'entreprise

[...]

Communication avec les autorités de contrôle et de contrôle

[...]

Documentation

44. L'auditeur doit consigner ce qui suit dans la documentation de l'audit⁹¹ portant sur ~~sa compréhension de l'entité et de son environnement et sur son~~ l'identification et l'évaluation des risques d'anomalies significatives exigées par la norme ISA 315 (révisée en 2019)⁹² :

- (a) les décisions importantes prises au cours des entretiens entre les membres de l'équipe affectés à la mission en ce qui concerne les possibilités d'anomalies significatives résultant de fraudes dans les états financiers de l'entité ;
- (b) les risques d'anomalies significatives résultant de fraudes identifiés et évalués au niveau des états financiers pris dans leur ensemble et au niveau des assertions ;
- (c) les contrôles identifiés de la composante « mesures de contrôle » qui visent à répondre aux risques d'anomalies significatives résultant de fraudes.

[...]

Modalités d'application et autres commentaires explicatifs

Caractéristiques de la fraude (Voir par. 3)

[...]

Esprit critique (Voir par. 12–14)

A7. Faire preuve d'esprit critique, c'est s'interroger tout au long de la mission sur la possibilité que les informations et les éléments probants recueillis donnent à penser qu'une anomalie significative résultant d'une fraude pourrait exister. L'esprit critique requiert également de s'interroger sur la fiabilité des informations à utiliser comme éléments probants et, ~~le cas échéant,~~ les contrôles identifiés de la composante « mesures de contrôle » (le cas échéant) portant sur la préparation et la mise à jour de ces informations. Compte tenu des caractéristiques de la fraude, il est particulièrement important que l'auditeur fasse preuve d'esprit critique lors de son évaluation des risques d'anomalies significatives résultant de fraudes.

[...]

Entretiens entre les membres de l'équipe affectés à la mission (Voir par. 15)

[...]

⁹¹ Norme ISA 230, *Documentation de l'audit*, paragraphes 8–11 et A6

⁹² Norme ISA 315 (révisée en 2019), paragraphe 3238

Procédures d'évaluation des risques et procédures liées

Demandes d'informations auprès de la direction

Évaluation par la direction des risques d'anomalies significatives résultant de fraudes (Voir par. 17 (a))

[...]

Demandes d'informations auprès de la fonction d'audit interne (Voir par. 19)

A18. La norme ISA 315 (révisée en 2019) et la norme ISA 610 (révisée en 2013) définissent des diligences et fournissent des indications pertinentes pour les audits des entités qui ont une fonction d'audit interne⁹³. Lors de la mise en œuvre des diligences de ces normes ISA en contexte de fraude, l'auditeur peut demander des informations au sujet d'activités spécifiques de la fonction, par exemple :

- quelles procédures ont été mises en œuvre par la fonction d'audit interne au cours de l'exercice, le cas échéant, pour détecter les fraudes ;
- si la direction a donné suite de façon satisfaisante aux constatations découlant de l'application de ces procédures.

Prise de connaissance de la surveillance exercée par les personnes constituant le gouvernement d'entreprise (Voir par. 20)

A19. Les personnes constituant le gouvernement d'entreprise de l'entité exercent une surveillance sur les systèmes de suivi des risques, du contrôle financier et de la conformité à la législation. Dans beaucoup de pays, les pratiques en matière de gouvernance sont bien développées et les personnes constituant le gouvernement d'entreprise jouent un rôle actif dans la surveillance de l'évaluation des risques de fraude par l'entité et ~~du contrôle interne relatif des contrôles visant à répondre à ces~~ risques. Étant donné que les responsabilités qui incombent aux personnes constituant le gouvernement d'entreprise et à la direction peuvent varier selon l'entité et d'un pays à l'autre, il est important que l'auditeur comprenne la nature de leurs responsabilités respectives pour pouvoir prendre connaissance de la surveillance exercée par les personnes compétentes⁹⁴.

A20. La connaissance de la surveillance exercée par les personnes constituant le gouvernement d'entreprise peut éclairer l'auditeur sur les possibilités que l'entité soit exposée à des fraudes commises par la direction, sur le caractère adéquat ~~du contrôle interne relatif aux des contrôles visant à répondre à ces~~ risques de fraude et sur la compétence et l'intégrité de la direction. L'auditeur peut acquérir cette connaissance par différents moyens, par exemple en assistant à des réunions au cours desquelles ces questions sont abordées, par la lecture des procès-verbaux de ces réunions, ou encore par des demandes d'informations auprès des personnes constituant le gouvernement d'entreprise.

Considérations propres aux petites entités

⁹³ Norme ISA 315 (révisée en 2019), par. 614 a) et sous-par. 24 (a)(ii) paragraphe 23, et norme ISA 610 (révisée en 2013), *Utilisation des travaux des auditeurs internes*.

⁹⁴ Les paragraphes A1–A8 de la norme ISA 260 (révisée) expliquent avec qui l'auditeur communique lorsque la structure de gouvernance de l'entité n'est pas bien définie.

[...]

Prise en considération d'autres informations (Voir par. 23)

A22. En plus des informations obtenues par la mise en œuvre de procédures analytiques, d'autres informations recueillies au sujet de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité peuvent être utiles pour identifier les risques d'anomalies significatives résultant de fraudes. Les entretiens entre les membres de l'équipe affectés à la mission peuvent fournir des informations utiles pour l'identification de ces risques. Les informations obtenues par l'auditeur dans le cadre du processus d'acceptation ou de maintien de la relation client, de même que l'expérience acquise lors d'autres missions réalisées pour l'entité, par exemple des missions d'examen d'informations financières intermédiaires, peuvent aussi se révéler pertinentes pour l'identification des risques d'anomalies significatives résultant de fraudes.

Évaluation des facteurs de risque de fraude (Voir par. 24)

[...]

A25. L'Annexe 1 présente des exemples de facteurs de risque de fraude ayant rapport aux informations financières mensongères et aux détournements d'actifs. Ces exemples sont classés en fonction des trois conditions généralement présentes en cas de fraude :

- des motifs ou des pressions pour commettre une fraude ;
- des circonstances perçues comme favorables à la perpétration d'une fraude ;
- la capacité de rationaliser l'acte frauduleux.

Les facteurs de risque de fraude peuvent être liés à des motifs, à des pressions ou à des circonstances favorables découlant de situations qui donnent lieu à une possibilité d'anomalies avant prise en considération des contrôles. Dans la mesure où ils influent sur le risque inhérent, les facteurs de risque de fraude, dont les biais introduits intentionnellement par la direction, constituent des facteurs de risque inhérent⁹⁵. Les facteurs de risque de fraude peuvent aussi être rattachés à des conditions, présentes dans le système de contrôle interne de l'entité, qui offrent l'occasion de commettre une fraude ou qui sont susceptibles d'influencer l'attitude de la direction ou sa capacité à justifier l'acte frauduleux. Il se peut que les facteurs de risque de fraude qui reflètent une attitude permettant la rationalisation de l'acte frauduleux ne soient pas facilement décelables par l'auditeur. Il peut néanmoins arriver qu'il prenne connaissance de l'existence de telles d'informations indiquant la présence de tels facteurs, notamment grâce à la connaissance qu'il est tenu d'acquérir de l'environnement de contrôle de l'entité⁹⁶. Bien que les facteurs de risque de fraude décrits à l'Annexe 1 couvrent un large éventail de situations susceptibles d'être rencontrées par l'auditeur, ils ne constituent que des exemples, et d'autres facteurs de risque peuvent exister.

[...]

Identification et évaluation des risques d'anomalies significatives résultant de fraudes

⁹⁵ Norme ISA 315 (révisée en 2019), par. 12 (f)

⁹⁶ Norme ISA 315 (révisée en 2019), paragraphe 21

Risques de fraude dans la comptabilisation des produits (Voir par. 26)

[...]

Identification et évaluation des risques d'anomalies significatives résultant de fraudes, et connaissance des contrôles correspondants de l'entité (Voir par. 27)

A31. La direction peut être amenée à porter des jugements sur la nature et l'étendue des contrôles qu'elle choisit de mettre en œuvre et sur la nature et l'étendue des risques qu'elle décide d'assumer. Pour déterminer les types de contrôles à mettre en œuvre dans le but de prévenir et de détecter les fraudes, la direction prend en compte les risques que les états financiers puissent comporter des anomalies significatives résultant de fraudes. Dans sa démarche, la direction peut être amenée à conclure qu'il n'est pas efficace par rapport au coût de mettre en œuvre et de maintenir un contrôle particulier lorsque la réduction attendue des risques d'anomalies significatives résultant de fraudes est limitée.

A32. Il est donc important pour l'auditeur de prendre connaissance des contrôles conçus, mis en œuvre et maintenus par la direction pour prévenir et détecter les fraudes. ~~Ce faisant~~ En identifiant les contrôles qui visent à répondre aux risques d'anomalies significatives résultant de fraudes, l'auditeur peut constater, par exemple, que la direction a sciemment accepté les risques associés à une non-séparation des tâches. Par ailleurs, les informations obtenues dans le cadre de ~~l'acquisition de cette compréhension~~ l'identification de ces contrôles, de l'évaluation de leur conception et de la vérification de leur mise en œuvre peuvent également être utiles pour identifier les facteurs de risque de fraude susceptibles d'avoir une incidence sur l'évaluation par l'auditeur des risques que les états financiers comportent des anomalies significatives résultant de fraudes.

Réponses à l'évaluation des risques d'anomalies significatives résultant de fraudes

Approche générale (Voir par. 28)

[...]

Affectation et supervision de l'équipe affectés à la mission (Voir par. 29 (a))

[...]

Élément d'imprévisibilité dans le choix des procédures d'audit (Voir par. 29 (c))

[...]

Procédures d'audit en réponse à l'évaluation des risques d'anomalies significatives résultant de fraudes au niveau des assertions (Voir par. 30)

[...]

Procédures d'audit en réponse aux risques de contournement des contrôles par la direction

Écritures comptables et autres ajustements (Voir par. 32 (a))

[...]

- A42. En outre, il importe que l'auditeur considère les risques d'anomalies significatives liés au contournement des contrôles sur les écritures comptables⁹⁷, car si les processus et les contrôles automatisés peuvent réduire le risque d'erreurs accidentelles, ils n'éliminent pas le risque que des personnes contournent ces processus automatisés, par exemple en modifiant les montants qui sont automatiquement transmis au grand livre ou au système d'information financière. Dans les cas où on a recours à l'informatique pour le transfert automatique d'informations, il se peut aussi qu'il y ait peu ou point de traces visibles de telles interventions dans les systèmes d'information.
- A43. Pour identifier et sélectionner les écritures comptables et les autres ajustements à tester, et afin de déterminer la méthode appropriée pour examiner les pièces justificatives des éléments sélectionnés, les facteurs suivants sont pertinents :
- *l'identification et l'évaluation des risques d'anomalies significatives résultant de fraudes* — la présence de facteurs de risque de fraude et les autres informations recueillies dans le cadre de l'identification et de l'évaluation des risques d'anomalies significatives résultant de fraudes peuvent aider l'auditeur à identifier des catégories spécifiques d'écritures comptables et d'autres ajustements à tester ;
 - *les contrôles mis en œuvre sur les écritures comptables et les autres ajustements* — la mise en œuvre de contrôles efficaces sur la préparation et la passation des écritures comptables et des autres ajustements peut permettre de réduire l'étendue des contrôles de substance à mettre en œuvre, à condition que l'auditeur ait testé l'efficacité du fonctionnement des contrôles ;
 - *le processus d'information financière de l'entité et la nature des éléments probants pouvant être recueillis* — dans de nombreuses entités, le traitement des opérations courantes comporte des contrôles tâches et des procédures à la fois manuelles et automatisées manuels et automatisés. De la même façon, le traitement des écritures comptables et des autres ajustements peut comporter des procédures et des contrôles à la fois manuels et automatisés. Dans les cas où l'informatique est utilisée dans le processus d'information financière, il se peut que les écritures comptables et les autres ajustements n'existent que sur support électronique ;
 - *les caractéristiques des écritures comptables et des autres ajustements frauduleux* — les écritures comptables et les autres ajustements incorrects présentent souvent des caractéristiques particulières. Il peut notamment s'agir d'écritures (a) enregistrées dans des comptes sans lien entre eux, inhabituels ou rarement utilisés, (b) passées par des personnes qui ne sont pas censées enregistrer d'écritures, (c) inscrites en fin de période ou après la date de clôture avec peu ou pas de justification ou de description, (d) passées sans numéro de compte soit avant ou pendant la préparation des états financiers, ou (e) comportant des chiffres ronds ou qui se terminent invariablement par les mêmes chiffres ;
 - *la nature et la complexité des comptes* — les écritures comptables et les autres ajustements incorrects peuvent être enregistrés dans des comptes qui (a) comportent des opérations complexes ou de nature inhabituelle, (b) contiennent des estimations et des ajustements de clôture importants, (c) ont comporté des anomalies dans le passé, (d) n'ont pas fait l'objet d'un rapprochement dans le délai normal ou comportent des différences non expliquées, (e) contiennent des opérations intragroupe, ou (f) sont associés d'une façon ou d'une autre à un risque

⁹⁷ Norme ISA 315 (révisée en 2019), sous-par. 26 (a)(ii).

identifié d'anomalies significatives résultant de fraudes. Lors de l'audit d'entités ayant plusieurs établissements ou composantes, il faut envisager la nécessité de sélectionner des écritures comptables de plusieurs établissements ;

- *les écritures comptables et les autres ajustements traités hors du cadre normal des activités* — il se peut que les contrôles auxquels sont soumises les écritures comptables non standard ne soient pas de même nature et de même étendue soumises au même niveau de contrôle interne que les contrôles auxquels sont soumises les écritures comptables courantes passées pour enregistrer des opérations telles que les ventes, les achats et les décaissements mensuels.

[...]

Estimations comptables (Voir par. 32 (b))

[...]

Justification économique des opérations importantes (Voir par. 32 (c))

[...]

Évaluation des éléments probants (Voir par. 34–37)

[...]

Procédures analytiques mises en œuvre vers la fin de l'audit pour parvenir à une conclusion générale (Voir par. 34)

[...]

Prise en compte des anomalies détectées (Voir par. 35–37)

[...]

Impossibilité de poursuivre la mission (Voir par. 38)

[...]

Déclarations écrites (Voir par. 39)

[...]

Communication avec la direction et avec les personnes constituant le gouvernement d'entreprise

Communication avec la direction (Voir par. 40)

[...]

Communication avec les personnes constituant le gouvernement d'entreprise (Voir par. 41)

[...]

Autres questions ayant trait à la fraude (Voir par. 42)

[...]

Communication avec les autorités de contrôle et de contrôle (Voir par. 43)

[...]

Annexe 1
(Voir par. A25)

Exemples de facteurs de risque de fraude

La présente annexe contient des exemples de facteurs de risque de fraude que peuvent rencontrer les auditeurs dans des situations très variées. Elle présente séparément les exemples ayant trait aux deux types de fraudes pris en considération par l'auditeur : les informations financières mensongères et les détournements d'actifs. Pour chacun de ces types de fraudes, les facteurs de risque sont par ailleurs classés selon les trois conditions qui sont généralement présentes en cas d'anomalies significatives résultant de fraudes, soit : (a) motifs et pressions, (b) circonstances favorables et (c) attitudes et rationalisations. Bien que les facteurs de risque présentés couvrent un large éventail de situations, il ne s'agit que d'exemples ; en conséquence, l'auditeur peut identifier d'autres facteurs de risque ou des facteurs différents. Tous les exemples cités ne sont pas applicables à toutes les situations rencontrées, et certains d'entre eux peuvent avoir plus ou moins d'importance selon la taille de l'entité, son mode de propriété ou les circonstances. Enfin, l'ordre dans lequel les facteurs sont présentés ne reflète pas leur importance relative ou leur fréquence de survenance.

Les facteurs de risque de fraude peuvent être liés à des motifs, à des pressions ou à des circonstances favorables découlant de situations qui donnent lieu à une possibilité d'anomalies avant prise en considération des contrôles (à savoir, le risque inhérent). De tels facteurs constituent des facteurs de risque inhérent, dans la mesure où ils influent sur le risque inhérent, et peuvent résulter de biais introduits par la direction. Par ailleurs, il se peut que des facteurs de risque de fraude liés à des circonstances favorables découlent d'autres facteurs de risque inhérent (par exemple, la complexité ou l'incertitude peuvent créer des circonstances favorables qui, à leur tour, peuvent donner lieu à une possibilité d'anomalies résultant de fraudes). Les facteurs de risque de fraude liés à des circonstances favorables peuvent aussi être rattachés à des conditions présentes dans le système de contrôle interne de l'entité, telles que des limites ou des déficiences dans le contrôle interne de l'entité qui créent de telles circonstances. Quant aux facteurs de risque de fraude liés aux comportements et aux justifications, ils découlent dans bien des cas de limites ou de déficiences de l'environnement de contrôle de l'entité.

Facteurs de risque associés à des anomalies résultant d'informations financières mensongères

Les exemples de facteurs de risque qui suivent sont associés à des anomalies résultant d'informations financières mensongères.

Motifs et pressions

La stabilité financière ou la rentabilité de l'entité sont menacées par des conditions économiques ou sectorielles ou par des conditions affectant l'exploitation de l'entité, telles que les suivantes :

[...]

La direction subit des pressions énormes pour satisfaire aux diligences ou aux attentes de tiers en raison :

[...]

Les informations disponibles indiquent que les performances financières de l'entité menacent la situation financière personnelle des dirigeants ou des personnes constituant le gouvernement d'entreprise du fait :

[...]

Circonstances favorables

La nature des activités de l'entité ou du secteur fournit des occasions de présenter des informations financières mensongères en raison des faits suivants :

[...]

Le suivi de la direction n'est pas efficace, pour les raisons suivantes :

[...]

La structure organisationnelle est complexe ou instable, comme l'attestent les faits suivants :

[...]

~~Des composantes du~~ Le contrôle interne ~~est~~ comporte des déficiences pour les raisons suivantes :

- le recours à un processus inadéquat pour le suivi ~~inadéquat~~ du système de contrôle interne de l'entité des contrôles, y compris les contrôles automatisés et les contrôles sur l'information financière intermédiaire (lorsque la publication externe de celle-ci est requise) ;
- des taux de rotation élevés ou l'emploi de personnel inefficace dans les fonctions de comptabilité, d'informatique ou d'audit interne ;
- des systèmes comptables et d'information inefficaces, notamment des situations impliquant des déficiences importantes du contrôle interne.

Attitudes et rationalisations

[...]

Facteurs de risque associés à des anomalies résultant de détournements d'actifs

Les facteurs de risque associés à des anomalies résultant de détournements d'actifs sont également classés selon les trois conditions généralement présentes en cas de fraude : les motifs et les pressions, les circonstances favorables, ainsi que les attitudes et les rationalisations. Certains des facteurs de risque associés à des anomalies résultant d'informations financières mensongères peuvent aussi être présents dans le cas d'anomalies résultant de détournements d'actifs. Par exemple, il peut y avoir un suivi inefficace exercé sur la direction ou d'autres déficiences dans le contrôle interne dans le cas d'anomalies résultant d'informations financières mensongères ou de détournements d'actifs. On trouvera ci-après une liste d'exemples de facteurs de risque de fraude associés à des anomalies résultant de détournements d'actifs.

Motifs et pressions

[...]

Circonstances favorables

Certaines caractéristiques ou circonstances peuvent accroître le risque de détournements d'actifs.

Par exemple, les facteurs suivants augmentent les possibilités de détournements d'actifs :

[...]

~~Un~~ Des contrôles interne ~~inadéquats~~ sur certains actifs peuvent accroître le risque de détournements de ces actifs. Par exemple, des détournements d'actifs peuvent survenir pour les raisons suivantes :

- séparation des tâches ou contrôles indépendants inadéquats ;
- surveillance inadéquate des dépenses de la haute direction, notamment les frais de déplacement et autres frais remboursés ;
- surveillance inadéquate, par la direction, du personnel responsable des actifs (par exemple, supervision ou suivi inadéquats des établissements éloignés) ;
- sélection inadéquate des candidats aux postes donnant accès à des actifs ;
- tenue inadéquate des fichiers sur les actifs ;
- système d'autorisation et d'approbation des opérations inadéquat (par exemple, pour les achats) ;
- moyens inadéquats de protection physique des espèces, des titres, des stocks ou des immobilisations ;
- absence de rapprochements exhaustifs et en temps opportun des actifs ;
- manque de documentation appropriée et en temps opportun pour certaines opérations (par exemple, dans le cas des crédits pour retours de marchandises) ;
- absence de vacances obligatoires pour le personnel exécutant des fonctions clés en matière de contrôle ;
- connaissance insuffisante de l'informatique de la part de la direction, ce qui donne la possibilité au personnel informatique de commettre des détournements ;
- contrôles d'accès inadéquats sur les fichiers automatisés, y compris les contrôles sur les journaux de bord des systèmes informatiques et l'analyse de ces journaux.

Attitudes et rationalisations

- Indifférence concernant le besoin de contrôler ou de réduire les risques liés au détournement d'actifs.
- Indifférence concernant les contrôles interne ~~relatifs~~ aux détournements d'actifs (contournement des contrôles existants ou absence de mesures appropriées pour corriger les déficiences connues du contrôle interne).
- Comportement dénotant du mécontentement ou de l'insatisfaction par rapport à l'entité ou à la façon dont elle traite l'employé.
- Changement de comportement ou de train de vie pouvant constituer un indice de détournements d'actifs.
- Tolérance pour les petits vols.

Annexe 2
(Voir par. A40)

Exemples de procédures d'audit possibles en réponse à l'évaluation des risques d'anomalies significatives résultant de fraudes

On trouvera ci-après une liste d'exemples de procédures d'audit qu'il est possible de mettre en œuvre en réponse à l'évaluation des risques d'anomalies significatives résultant de fraudes associées à des informations financières mensongères et à des détournements d'actifs. Bien que les procédures indiquées couvrent un large éventail de situations, elles ne constituent que des exemples et, par conséquent, peuvent ne pas être les plus appropriées ou ne pas être nécessaires dans toutes les situations. Enfin, l'ordre dans lequel les procédures sont présentées ne reflète pas leur importance relative.

Prise en considération des risques au niveau des assertions

Les réponses spécifiques de l'auditeur à son évaluation des risques d'anomalies significatives résultant de fraudes varient selon les types ou les associations de facteurs de risque de fraude ou de conditions identifiés, et selon les flux d'opérations, les soldes de comptes, les informations à fournir et les assertions susceptibles d'être affectés.

Voici des exemples de réponses spécifiques de l'auditeur :

[...]

- lorsque les travaux d'un expert deviennent particulièrement importants relativement à un poste des états financiers pour lequel le risque d'anomalies significatives résultant de fraudes est considéré comme élevé, mettre en œuvre des procédures supplémentaires portant sur certaines ou l'ensemble des hypothèses, méthodes ou constatations de l'expert pour s'assurer que les constatations de celui-ci ne sont pas déraisonnables, ou engager un autre expert à cette fin ;

[...]

Réponses spécifiques — Anomalies résultant d'informations financières mensongères

Voici des exemples de réponses de l'auditeur à son évaluation des risques d'anomalies significatives résultant d'informations financières mensongères :

Annexe 3
(Voir par. A49)

Exemples de situations qui indiquent la possibilité de fraudes

La liste ci-après donne des exemples de situations qui peuvent indiquer la possibilité que les états financiers comportent une anomalie significative résultant de fraudes.

[...]

Norme ISA 300, *Planification d'un audit d'états financiers*

Modalités d'application et autres commentaires explicatifs

[...]

Documentation (Voir par. 12)

[...]

Considérations propres aux petites entités

A21. Comme il est indiqué au paragraphe A11, un bref mémorandum au dossier est parfois suffisant pour consigner la stratégie d'audit dans le cas d'une petite entité. Pour ce qui concerne le programme de travail, il est possible d'utiliser des programmes d'audit standard ou des listes de contrôle standard (voir le paragraphe A19) conçus en supposant que les contrôles ~~mesures de contrôle~~⁹⁸ ~~pertinentes~~ sont peu nombreux ~~ses~~ – comme c'est vraisemblablement le cas dans une petite entité – pourvu qu'ils soient adaptés aux circonstances de la mission, notamment au résultat de l'évaluation des risques par l'auditeur.

[...]

Norme ISA 402, *Facteurs à considérer pour l'audit d'entités faisant appel à une société de services*

Introduction

Champ d'application de la présente norme ISA

1. La présente norme internationale d'audit (ISA) traite de la responsabilité qui incombe à l'auditeur de recueillir des éléments probants suffisants et appropriés lorsque l'entité auditée (l'entité utilisatrice) a recours à une ou plusieurs sociétés de services. Plus spécifiquement, elle fournit des précisions sur la façon dont l'auditeur de l'entité utilisatrice applique la norme ISA 315 (révisée en 2019) et la norme ISA 330 pour prendre connaissance de l'entité utilisatrice, notamment ainsi que des aspects de son système de contrôle interne qui sont pertinents pour l'audit la préparation des états financiers, qui soit suffisante pour lui permettre d'identifier et d'évaluer les risques d'anomalies significatives et de concevoir et mettre en œuvre des procédures d'audit complémentaires en réponse à ces risques.

[...]

3. Les prestations d'une société de services sont pertinentes pour l'audit des états financiers d'une entité utilisatrice lorsque les prestations fournies, ainsi que les contrôles exercés sur celles-ci, font partie du système d'information de l'entité utilisatrice (~~y compris les processus opérationnels connexes~~) pertinent pour l'information financière la préparation des états financiers. ~~Bien qu'il y ait de bonnes chances que la plupart des contrôles de la société de services aient rapport à l'information financière fassent partie de ce système, ou des il se peut que d'autres contrôles y afférents soient pertinents pour l'audit~~, notamment ceux mis en œuvre pour la sauvegarde des actifs. Les prestations

⁹⁸ Norme ISA 315 (révisée en 2019), par. 26 (a)

fournies par la société de services font partie du système d'information de l'entité utilisatrice (~~y compris les processus opérationnels connexes~~) pertinent pour l'information financière si elles concernent l'un quelconque des éléments suivants :

- (a) le flux, dans le système d'information de l'entité utilisatrice, des informations relatives aux flux d'opérations importants, aux soldes de comptes importants et aux informations à fournir importantes, peu importe que les étapes soient effectuées manuellement ou à l'aide de l'informatique, et peu importe la provenance de ces informations (grand livre et journaux auxiliaires, ou autre). Les flux d'opérations conclues dans le cadre des activités de l'entité utilisatrice qui sont importantes par rapport aux états financiers de celle-ci ; Cela comprend les prestations fournies par la société de services qui influent sur la façon :
 - (i) ~~b) les procédures suivies, tant dans les systèmes informatisés que dans les systèmes manuels, pour le déclenchement, l'enregistrement, le traitement, la correction au besoin, le report au grand livre général et la communication dans les états financiers des opérations de l'entité utilisatrice ; dont les opérations de l'entité utilisatrice sont déclenchées et dont les informations les concernant sont initiées, enregistrées, traitées, corrigées si nécessaire, reportées au grand livre et présentées dans les états financiers ;~~
 - (ii) dont les informations sur des événements ou des situations, autres que les opérations, sont saisies, traitées et fournies par l'entité utilisatrice dans les états financiers ;
- (b) ~~(e) les documents comptables connexes, sur support électronique ou papier, les informations justificatives et les comptes spécifiques~~ contenus dans les des états financiers de l'entité utilisatrice et les autres documents justificatifs qui concernent le flux des informations décrit au paragraphe 3 a) qui servent au déclenchement, à l'enregistrement, au traitement et à la communication des opérations de l'entité utilisatrice, ce qui comprend la correction des informations erronées et la manière dont les informations sont reportées au grand livre général ;
- (d) ~~la façon dont le système d'information de l'entité utilisatrice saisit les événements et situations, autres que les opérations, qui ont de l'importance pour les états financiers ;~~
- (c) ~~(e) le processus d'information financière utilisé pour préparer les états financiers de l'entité utilisatrice à partir des documents comptables mentionnés au paragraphe 3 b), y compris en ce qui concerne les informations à fournir et les estimations comptables se rapportant à des flux d'opérations les estimations comptables importantes, à des soldes de comptes importants et à des informations à fournir importantes et les informations importantes à fournir ;~~
- (d) l'environnement informatique de l'entité qui est pertinent au regard des points (a)–(c) ci-dessus.
- (f) ~~les contrôles afférents aux écritures de journal, y compris les écritures non courantes servant à constater les opérations ou ajustements non récurrents ou inhabituels.~~

[...]

Objectifs

7. Les objectifs de l'auditeur d'une entité utilisatrice qui fait appel aux prestations d'une société de services sont :

- (a) de prendre connaissance de la nature et de l'importance des prestations fournies par la société de services ainsi que de leur ~~effet incidence sur les aspects du système de~~ contrôle interne de l'entité utilisatrice pertinents pour l'audit, qui soit suffisante pour lui ~~permettre d'identifier et d'évaluer les~~ fournir une base appropriée aux fins de l'identification et de l'évaluation des risques d'anomalies significatives ;
- (b) de concevoir et de mettre en œuvre des procédures d'audit en réponse à ces risques.

[...]

Diligences

Prise de connaissance des prestations fournies par la société de services, y compris le contrôle interne

[...]

10. Pour prendre connaissance ~~des aspects du système de~~ contrôle interne de l'entité pertinents pour l'audit conformément à la norme ISA 315 (révisée en 2019)⁹⁹, l'auditeur de l'entité utilisatrice doit ~~évaluer la conception et la mise en place des contrôles pertinents identifier, au sein de l'entité utilisatrice, les contrôles de la composante « mesures de contrôle »¹⁰⁰ au sein de l'entité utilisatrice~~ qui ont rapport aux prestations fournies par la société de services, y compris ceux auxquels sont soumises les opérations traitées par la société de services. Il doit aussi évaluer la conception de ces contrôles et déterminer s'ils ont été mis en œuvre¹⁰¹. (Voir par. A12–A14)
11. L'auditeur de l'entité utilisatrice doit déterminer s'il a acquis une connaissance de la nature et de l'importance des prestations fournies par la société de services ~~et ainsi que de leur incidence sur les aspects du système de~~ contrôle interne de l'entité utilisatrice pertinents pour l'audit qui soit suffisante pour ~~pouvoir servir de lui fournir une base à appropriée aux fins de~~ l'identification et à de l'évaluation des risques d'anomalies significatives.
12. Si l'auditeur de l'entité utilisatrice n'est pas en mesure de prendre connaissance suffisante auprès de l'entité utilisatrice, il doit acquérir cette connaissance en mettant en œuvre une ou plusieurs des procédures suivantes :

[...]

- (c) visiter la société de services et mettre en œuvre des procédures qui fourniront les informations nécessaires sur ses contrôles pertinents ;
- (d) faire appel à un autre auditeur afin qu'il mette en œuvre des procédures qui fourniront les informations nécessaires sur les contrôles ~~pertinents~~ de la société de services. (Voir par. A15– A20)

Utilisation d'un rapport de type 1 ou de type 2 pour étayer la connaissance de la société de services acquise par l'auditeur de l'entité utilisatrice

⁹⁹ Norme ISA 315 (révisée), paragraphe 12

¹⁰⁰ Norme ISA 315 (révisée en 2019), par. 26 a)

¹⁰¹ Norme ISA 315 (révisée en 2019), par. 26 d)

[...]

14. Si l'auditeur de l'entité utilisatrice prévoit d'utiliser des informations contenues dans un rapport de type 1 ou de type 2 à titre d'éléments probants pour étayer sa connaissance de la conception et de la mise en œuvre des contrôles de la société de services, il doit :

[...]

- (b) évaluer le caractère suffisant et approprié des éléments probants fournis par le rapport pour permettre de comprendre les aspects des contrôles de la société de services interne de l'entité utilisatrice pertinents pour l'audit ;

[...]

Modalités d'application et autres commentaires explicatifs

Prise de connaissance des prestations fournies par la société de services, y compris le contrôle interne

[...]

Procédures complémentaires lorsqu'une connaissance suffisante ne peut être acquise auprès de l'entité utilisatrice (Voir par. 12)

[...]

- A19. Il est possible de faire appel à un autre auditeur afin qu'il mette en œuvre des procédures qui fourniront les informations nécessaires sur les contrôles pertinents de la société de services qui sont liés aux prestations fournies à l'entité utilisatrice. Lorsqu'un rapport de type 1 ou de type 2 a été délivré, l'auditeur de l'entité utilisatrice peut charger l'auditeur de la société de services de mettre en œuvre ces procédures, puisque ce dernier est déjà en relation avec la société de services. Les indications de la norme ISA 600 peuvent se révéler utiles pour l'auditeur de l'entité utilisatrice qui utilise les travaux d'un autre auditeur, car elles traitent de la connaissance de l'autre auditeur (notamment en ce qui a trait à son indépendance et à sa compétence professionnelle), de l'intervention dans les travaux de l'autre auditeur en ce qui concerne la planification de la nature, du calendrier et de l'étendue de ces travaux et de l'évaluation du caractère suffisant et approprié des éléments probants recueillis.

[...]

Utilisation d'un rapport de type 1 ou de type 2 pour étayer la connaissance de la société de services acquise par l'auditeur de l'entité utilisatrice (Voir par. 13–14)

[...]

- A22. Le rapport de type 1 ou de type 2 ainsi que les informations sur l'entité utilisatrice peuvent aider l'auditeur de l'entité utilisatrice à acquérir :

- (a) une connaissance des aspects des contrôles de la société de services qui peuvent avoir une incidence sur le traitement des opérations de l'entité utilisatrice, y compris le recours à des sous-traitants par la société de services ;
- (b) une connaissance du flux des opérations importantes au sein de la société de services pour déterminer les étapes du cheminement des opérations susceptibles d'entraîner des anomalies significatives dans les états financiers de l'entité utilisatrice ;
- (c) une connaissance des objectifs de contrôle de la société de services qui sont pertinents au regard des assertions contenues dans les états financiers de l'entité utilisatrice ;
- (d) une connaissance des contrôles de la société de services permettant de déterminer s'ils sont conçus et mis en œuvre de manière à prévenir ou à détecter les erreurs de traitement susceptibles d'entraîner des anomalies significatives dans les états financiers de l'entité utilisatrice.

Un rapport de type 1 ou de type 2 peut aider l'auditeur de l'entité utilisatrice à acquérir une connaissance suffisante pour lui permettre d'identifier et d'évaluer les risques d'anomalies significatives. Un rapport de type 1 ne fournit toutefois aucun élément probant quant à l'efficacité du fonctionnement des contrôles pertinents.

[...]

Réponses à l'évaluation des risques d'anomalies significatives (Voir par. 15)

[...]

Tests de procédures (Voir par. 16)

A29. La norme ISA 330 requiert de l'auditeur de l'entité utilisatrice qu'il conçoive et mette en œuvre des tests sur les contrôles pertinents de manière à recueillir des éléments probants suffisants et appropriés sur l'efficacité de leur fonctionnement dans certaines circonstances. Dans le cas d'une société de services, cette exigence s'applique :

[...]

A30. En l'absence de rapport de type 2, l'auditeur de l'entité utilisatrice peut communiquer avec la société de services, par l'entremise de l'entité utilisatrice, afin de demander que l'auditeur de la société de services prépare un rapport de type 2 comprenant des tests de l'efficacité du fonctionnement des contrôles pertinents, ou il peut avoir recours à un autre auditeur pour mettre en œuvre des procédures au sein de la société de services pour tester l'efficacité du fonctionnement de ces contrôles. L'auditeur de l'entité utilisatrice peut également visiter la société de services et effectuer les tests de procédures pertinents si la société de services y consent. Dans son évaluation des risques, l'auditeur de l'entité utilisatrice tient compte des éléments probants fournis tant par les travaux de l'autre auditeur que par les procédures qu'il a lui-même mises en œuvre.

Utilisation d'informations contenues dans d'un rapport de type 2 à titre d'éléments probants attestant que les contrôles de la société de services fonctionnent efficacement (Voir par. 17)

[...]

A33. Il peut également être nécessaire que l'auditeur de l'entité utilisatrice recueille des éléments probants additionnels sur les changements importants apportés aux contrôles ~~pertinents~~ de la société de services en dehors de la période couverte par le rapport de type 2 ou qu'il détermine des procédures d'audit supplémentaires à mettre en œuvre. Parmi les facteurs pertinents pour la détermination des éléments probants additionnels à recueillir sur les contrôles de la société de services qui fonctionnaient en dehors de la période couverte par le rapport de l'auditeur de la société de services, il y a les suivants :

[...]

- l'efficacité de l'environnement de contrôle et du processus de suivi du système des contrôles interne de par l'entité utilisatrice.

A34. Pour recueillir des éléments probants additionnels, l'auditeur peut par exemple étendre les tests de procédures sur la période restant à couvrir ou tester le processus de suivi du système des contrôles interne par qu'exerce l'entité utilisatrice.

[...]

A39. L'auditeur de l'entité utilisatrice est tenu de communiquer par écrit et en temps opportun à la direction et aux personnes constituant le gouvernement d'entreprise les déficiences importantes relevées au cours de l'audit¹¹. L'auditeur de l'entité utilisatrice doit également communiquer en temps opportun à la direction, au niveau hiérarchique approprié, les autres déficiences dans contrôle interne relevées au cours de l'audit qui sont suffisamment préoccupantes, selon son jugement professionnel, pour nécessiter l'attention de la direction¹². Les questions que l'auditeur de l'entité utilisatrice peut relever au cours de l'audit et souhaiter communiquer à la direction et aux personnes constituant le gouvernement d'entreprise de l'entité utilisatrice comprennent :

- tout ~~suivi des contrôles~~ qui fait partie du processus de suivi du système de contrôle interne par l'entité et qui pourrait être mis en œuvre par l'entité utilisatrice, y compris ceux identifiés par suite de l'obtention d'un rapport de type 1 ou de type 2 ;

[...]

Norme ISA 330, Réponses de l'auditeur à l'évaluation des risques

Introduction

Champ d'application de la présente norme ISA

1. La présente norme internationale d'audit (ISA) traite de la responsabilité qui incombe à l'auditeur de concevoir et de mettre en œuvre des réponses à l'évaluation des risques d'anomalies significatives qu'il a effectuée conformément à la norme ISA 315 (révisée en 2019)¹⁰² dans le cadre d'un audit d'états financiers.

¹⁰² Norme ISA 315 (révisée en 2019), *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives*.

Date d'entrée en vigueur

2. La présente norme ISA s'applique aux audits d'états financiers des périodes ouvertes à compter du 15 décembre 2009.

Objectif

3. L'objectif de l'auditeur est de concevoir et de mettre en œuvre des réponses adaptées à l'évaluation des risques d'anomalies significatives afin de recueillir des éléments probants suffisants et appropriés sur ces risques.

Définitions

4. Dans les normes ISA, on entend par :
 - (a) « procédure de corroboration », une procédure d'audit conçue pour détecter des anomalies significatives au niveau des assertions. Les contrôles de substance comprennent :
 - (i) des tests de détail (relatifs à un flux d'opérations, à un solde de compte ou à une information fournie),
 - (ii) des procédures analytiques de substance ;
 - (b) « test des procédures », une procédure d'audit conçue pour évaluer l'efficacité du fonctionnement des contrôles visant à prévenir, ou à détecter et corriger, les anomalies significatives au niveau des assertions.

Diligences

Approche générale

5. L'auditeur doit concevoir et mettre en œuvre une approche générale adaptée à son évaluation des risques d'anomalies significatives au niveau des états financiers. (Voir par. A1–A3)

Procédures d'audit en réponse à l'évaluation des risques d'anomalies significatives au niveau des assertions

6. L'auditeur doit concevoir et mettre en œuvre des procédures d'audit complémentaires dont la nature, le calendrier et l'étendue sont fonction de son évaluation des risques d'anomalies significatives au niveau des assertions. (Voir par. A4–A8 et A42–A52)
7. Pour concevoir les procédures d'audit complémentaires à mettre en œuvre, l'auditeur doit :
 - (a) tenir compte des raisons qui sous-tendent l'évaluation du risque d'anomalies significatives au niveau des assertions pour chaque catégorie d'opérations importante, chaque solde de compte important et chaque information ~~fournie~~ à fournir importante, y compris :

- (i) la probabilité et l'ampleur des d'anomalies ~~significatives~~ compte tenu des caractéristiques particulières de la catégorie d'opérations importante, du solde de compte important ou de l'information ~~fournie à fournir importante~~ (c'est-à-dire le risque inhérent),
 - (ii) la prise en compte ou non, dans l'évaluation du risque, des contrôles ~~pertinents~~ visant à répondre au risque d'anomalies significatives (c'est-à-dire le risque lié au contrôle interne), leur prise en compte requérant l'obtention par l'auditeur d'éléments probants lui permettant de déterminer si les contrôles fonctionnent efficacement (lorsqu'il ~~a l'intention de s'appuyer sur~~ prévoit de tester l'efficacité du fonctionnement des contrôles pour déterminer la nature, le calendrier et l'étendue des contrôles de substance) ; (Voir par. A9–A18)
- (b) recueillir des éléments probants d'autant plus convaincants que, selon son évaluation, le risque est considéré comme élevé. (Voir par. A19)

Test des contrôles

8. L'auditeur doit concevoir et mettre en œuvre des tests sur les contrôles ~~pertinents~~ de manière à recueillir des éléments probants suffisants et appropriés sur l'efficacité de leur fonctionnement dans l'un ou l'autre des cas suivants :
- (a) son évaluation des risques d'anomalies significatives au niveau des assertions repose sur l'attente d'un fonctionnement efficace des contrôles (c'est-à-dire qu'il ~~a l'intention de s'appuyer sur~~ prévoit de tester l'efficacité du fonctionnement des contrôles pour déterminer la nature, le calendrier et l'étendue des contrôles de substance) ;
 - (b) les contrôles de substance ne permettent pas à eux seuls de recueillir des éléments probants suffisants et appropriés au niveau des assertions. (Voir par. A20–A24)
9. Lors de la conception et de la mise en œuvre des tests de procédures, l'auditeur doit recueillir des éléments probants d'autant plus convaincants qu'il s'appuie sur l'efficacité des contrôles. (Voir par. A25)

Nature et étendue des tests de procédures

10. Lors de la conception et de la mise en œuvre des tests de procédures, l'auditeur doit :
- (a) mettre en œuvre d'autres procédures d'audit en association avec des demandes d'informations afin de recueillir des éléments probants attestant l'efficacité du fonctionnement des contrôles, et notamment :
 - (i) la façon dont les contrôles ont été appliqués à des moments pertinents pendant la période auditée,
 - (ii) s'ils ont été appliqués systématiquement,
 - (iii) par qui ou par quels moyens ils ont été appliqués ; (Voir par. A26–A29a)

- (b) déterminer, dans la mesure où cela n'a pas déjà été fait, si les contrôles à tester dépendent ~~sont tributaires~~ d'autres contrôles (contrôles indirects) et, dans l'affirmative, s'il est nécessaire de recueillir des éléments probants attestant l'efficacité du fonctionnement de ces contrôles indirects. (Voir par. A30–A31)

Calendrier des tests de procédures

11. L'auditeur doit tester l'efficacité du fonctionnement des contrôles pour le moment précis ou pour l'ensemble de la période où il a l'intention de s'appuyer sur ces contrôles, sous réserve des dispositions des paragraphes 12 et 15 ci-dessous, afin de disposer d'une base appropriée pour justifier son intention de s'appuyer sur les contrôles. (Voir par. A32)

Utilisation d'éléments probants recueillis au cours d'une période intermédiaire

12. Si l'auditeur recueille des éléments probants quant à l'efficacité du fonctionnement des contrôles au cours d'une période intermédiaire, il doit :
- (a) recueillir des éléments probants concernant tout changement important survenu dans ces contrôles après la période intermédiaire ;
 - (b) déterminer les éléments probants additionnels à obtenir pour la période restant à couvrir jusqu'à la fin de l'exercice. (Voir par. A33–A34)

Utilisation d'éléments probants recueillis au cours des audits précédents

13. Pour déterminer s'il est approprié d'utiliser des éléments probants sur l'efficacité du fonctionnement des contrôles recueillis lors des audits précédents et, lorsque c'est le cas, pour déterminer le délai maximal pouvant s'écouler avant de procéder à un nouveau test sur un contrôle, l'auditeur doit tenir compte des éléments suivants :
- (a) l'efficacité des autres ~~éléments~~ composantes du système de contrôle interne de l'entité, notamment l'environnement de contrôle, le processus de suivi du système des contrôles interne par l'entité et le processus d'évaluation des risques par l'entité ;
 - (b) les risques découlant des caractéristiques du contrôle considéré, notamment selon qu'il est manuel ou automatisé ;
 - (c) l'efficacité des contrôles généraux sur les systèmes informatiques ;
 - (d) l'efficacité du contrôle considéré et son application par l'entité, y compris la nature et l'étendue des écarts constatés dans l'application du contrôle lors des audits précédents, ainsi que les changements de personnel ayant une incidence importante sur l'application du contrôle ;
 - (e) l'existence ou non d'un risque en raison de l'absence de changement dans le contrôle considéré alors que les circonstances ont changé ;
 - (f) les risques d'anomalies significatives et l'étendue de la confiance placée dans le contrôle considéré. (Voir par. A35)
14. Lorsque l'auditeur a l'intention d'utiliser des éléments probants recueillis lors d'un audit précédent et concernant l'efficacité et la fiabilité du fonctionnement de certains contrôles, il doit établir si ces éléments probants sont toujours pertinents en recueillant des éléments probants attestant si des

changements importants sont survenus ou non dans ces contrôles depuis l'audit précédent. Il obtient ces éléments probants au moyen de demandes d'informations en association avec des observations physiques ou des inspections, afin de confirmer sa connaissance de ces contrôles, et :

- (a) lorsque les éléments probants recueillis lors de l'audit précédent ont perdu de leur pertinence sous l'effet des changements survenus, l'auditeur doit tester les contrôles dans le cadre de l'audit en cours ; (Voir par. A36)
- (b) lorsqu'aucun changement n'est survenu, l'auditeur doit tester les contrôles au moins une fois tous les trois audits, mais doit tester une partie des contrôles lors de chaque audit afin d'éviter que tous les contrôles sur lesquels il a l'intention de s'appuyer soient testés au cours d'un même audit et qu'il s'écoule ensuite deux audits sans aucun test des contrôles. (Voir par. A37– A39)

Contrôles relatifs à des risques importants

15. Si l'auditeur a l'intention de s'appuyer sur des contrôles ~~liés~~ relatifs à un risque qu'il a jugé important, il doit tester ces contrôles dans la période sur laquelle porte sa mission.

Évaluation de l'efficacité du fonctionnement des contrôles

16. Lorsque l'auditeur évalue l'efficacité du fonctionnement des contrôles ~~pertinents sur lesquels il a l'intention de s'appuyer~~, il doit apprécier si les anomalies que les contrôles de substance ont permis de détecter indiquent que les contrôles ne fonctionnent pas efficacement. Le fait que les contrôles de substance n'aient permis de détecter aucune anomalie ne constitue toutefois pas un élément probant quant à l'efficacité des contrôles liés à l'assertion testée. (Voir par. A40)
17. Si des écarts dans l'application des contrôles sur lesquels l'auditeur a l'intention de s'appuyer sont détectés, il doit procéder à des demandes d'informations précises afin de comprendre la situation et ses conséquences potentielles, et il doit déterminer : (Voir par. A41)
 - (a) si les tests de procédures effectués procurent une base appropriée pour s'appuyer sur les contrôles ;
 - (b) si des tests additionnels des contrôles sont nécessaires ;
 - (c) si les risques ~~potentiels~~ d'anomalies significatives requièrent la mise en œuvre de contrôles de substance.

Contrôles de substance

18. Indépendamment de son évaluation des risques d'anomalies significatives, l'auditeur doit concevoir et mettre en œuvre des contrôles de substance pour chaque catégorie d'opérations significative, solde de compte significatif et information ~~fournie à fournir significative, dès lors qu'ils sont significatifs~~. (Voir par. A42–A47)
19. L'auditeur doit se demander s'il convient de mettre en œuvre des procédures de confirmation externe en tant que contrôles de substance. (Voir par. A48–A51)

Contrôles de substance liés au processus de finalisation des états financiers

20. Les contrôles de substance mis en œuvre par l'auditeur doivent comprendre les procédures suivantes liées au processus de finalisation des états financiers :
- (a) vérification de la concordance ou rapprochement des données communiquées dans les états financiers, y compris des informations fournies, avec les documents comptables sous-jacents, que celles-ci proviennent ou non du grand livre et des journaux auxiliaires ;
 - (b) examen des écritures comptables significatives et des autres ajustements effectués lors de la préparation des états financiers. (Voir par. A52)

Contrôles de substance en réponse aux risques importants

21. Si, lors de son évaluation, l'auditeur a déterminé que le risque d'anomalies significatives au niveau d'une assertion est important, il doit mettre en œuvre des contrôles de substance répondant spécifiquement à ce risque. Lorsque l'approche adoptée pour répondre à un risque important se limite à des contrôles de substance, ceux-ci doivent comporter des tests de détail. (Voir par. A53)

Calendrier des contrôles de substance

22. Si des contrôles de substance sont réalisés à une date intermédiaire, l'auditeur doit, pour couvrir le restant de la période, mettre en œuvre :
- (a) soit des contrôles de substance en association avec des tests de procédures,
 - (b) soit uniquement des contrôles de substance complémentaires, s'il juge que cela suffit,
- afin d'avoir une base raisonnable permettant d'extrapoler que les conclusions de l'audit à la date intermédiaire sont toujours valables à la fin de la période. (Voir par. A54–A57)
23. Lorsque l'auditeur détecte à une date intermédiaire des anomalies qu'il n'avait pas anticipées dans le cadre de son évaluation des risques d'anomalies significatives, il doit déterminer s'il est nécessaire de modifier son évaluation du risque concerné ainsi que la nature, le calendrier ou l'étendue prévus des contrôles de substance couvrant le restant de la période. (Voir par. A58)

Caractère adéquat de la présentation et des informations fournies

24. L'auditeur doit mettre en œuvre des procédures d'audit afin d'évaluer si la présentation d'ensemble des états financiers est conforme au référentiel comptable applicable. Pour faire cette évaluation, l'auditeur doit se demander si la présentation des états financiers traduit :
- le classement et la description appropriés des divers éléments de l'information financière et des opérations et événements sous-jacents ;
 - la présentation, la structure et le contenu appropriés des états financiers. (Voir par. A59)

Évaluation du caractère suffisant et approprié des éléments probants recueillis

25. En se fondant sur les procédures d'audit réalisées et les éléments probants recueillis, l'auditeur doit apprécier, avant de conclure l'audit, si les évaluations des risques d'anomalies significatives au niveau des assertions demeurent valables. (Voir par. A60–A61)
26. L'auditeur doit conclure sur le caractère suffisant et approprié des éléments probants recueillis. Pour se former une opinion, il doit tenir compte de tous les éléments probants pertinents, qu'ils semblent corroborer ou contredire les assertions contenues dans les états financiers. (Voir par. A62)
27. ~~Faute d'avoir recueilli des éléments probants suffisants et appropriés sur une assertion importante contenue dans les états financiers~~ en ce qui concerne une assertion pertinente portant sur un flux d'opérations, un solde de compte ou une information à fournir, l'auditeur doit chercher à recueillir des éléments probants complémentaires. S'il n'est pas en mesure de recueillir des éléments probants suffisants et appropriés, il doit exprimer une opinion avec réserve ou formuler une impossibilité d'exprimer une opinion sur les états financiers.

Documentation

28. L'auditeur doit consigner dans la documentation de l'audit¹⁰³ :
 - (a) l'approche générale adoptée par suite de son évaluation des risques d'anomalies significatives au niveau des états financiers ainsi que la nature, le calendrier et l'étendue des procédures d'audit complémentaires mises en œuvre ;
 - (b) le lien entre ces procédures et son évaluation des risques au niveau des assertions ;
 - (c) les résultats des procédures d'audit, y compris les conclusions lorsqu'elles ne ressortent pas clairement. (Voir par. A63)
29. Si l'auditeur a l'intention d'utiliser des éléments probants sur l'efficacité du fonctionnement des contrôles recueillis lors des audits précédents, il doit consigner dans la documentation de l'audit ses conclusions quant à la fiabilité des contrôles qui ont été testés lors d'un audit précédent.
30. La documentation de l'auditeur doit démontrer que les données communiquées dans les états financiers, y compris les informations fournies, concordent ou ont fait l'objet d'un rapprochement avec les documents comptables sous-jacents, que celles-ci proviennent ou non du grand livre et des journaux auxiliaires.

¹⁰³ Norme ISA 230, *Documentation de l'audit*, paragraphes 8–11 et A6.

Modalités d'application et autres commentaires explicatifs

Approche générale (Voir par. 5)

A1. Au titre d'approche générale à son évaluation des risques d'anomalies significatives au niveau des états financiers, l'auditeur peut notamment :

- insister auprès de l'équipe affectés à la mission sur la nécessité de garder un esprit critique ;
- affecter à la mission du personnel professionnel plus expérimenté ou possédant des compétences particulières, ou encore faire appel à des experts ;
- renforcer la supervision ~~modifier la nature, le calendrier et l'étendue de la direction et de la supervision des membres de l'équipe affectés à la mission, ainsi que de la revue de leurs travaux ;~~
- introduire un degré supplémentaire d'imprévisibilité lors du choix des procédures d'audit complémentaires à mettre en œuvre ;
- apporter des modifications à la stratégie générale d'audit, comme le requiert la norme ISA 300, ou aux procédures d'audit prévues, notamment en ce qui concerne :
 - la détermination par l'auditeur du seuil de planification conformément à la norme ISA 320,
 - les tests d'efficacité du fonctionnement des contrôles que l'auditeur a prévus et le caractère convaincant que devront présenter les éléments probants recueillis pour permettre à l'auditeur de s'appuyer sur l'efficacité du fonctionnement des contrôles, dans la mesure où il a l'intention de le faire, en particulier lorsque des déficiences ont été relevées dans l'environnement de contrôle ou dans les activités de suivi de l'entité,
 - la nature, le calendrier et l'étendue des contrôles de substance. Par exemple, il peut être approprié que ces contrôles soient mis en œuvre à la date de clôture, ou vers cette date, si les risques d'anomalies significatives sont élevés.
- ~~modifier globalement la nature, le calendrier ou l'étendue des procédures d'audit, notamment en mettant en œuvre des contrôles de substance à la fin de la période plutôt qu'à une date intermédiaire, ou en modifiant la nature des procédures d'audit afin d'obtenir des éléments probants plus convaincants.~~

A2. La connaissance qu'a l'auditeur de l'environnement de contrôle influe sur son évaluation du risque d'anomalies significatives au niveau des états financiers et sur l'approche générale qu'il adopte en conséquence de cette évaluation. Un environnement de contrôle efficace peut permettre à l'auditeur de faire davantage confiance au contrôle interne et à la fiabilité des éléments probants d'origine interne, ce qui peut l'amener par exemple à mettre en œuvre certaines procédures d'audit à une date intermédiaire plutôt qu'à la fin de la période. L'existence de déficiences dans l'environnement de contrôle produit l'effet inverse ; par exemple, en réponse à un environnement de contrôle inefficace, l'auditeur peut :

- concentrer davantage les procédures d'audit à la fin de la période plutôt qu'à une date intermédiaire ;
- chercher à obtenir plus d'éléments probants par la mise en œuvre de contrôles de substance ;
- augmenter le nombre d'établissements à inclure dans le champ de l'audit.

- A3. Ces considérations jouent donc un rôle important dans le choix d'une stratégie générale par l'auditeur, qui peut par exemple privilégier les contrôles de substance (stratégie de corroboration) ou une combinaison de tests de procédures et de contrôles de substance (stratégie mixte).

Procédures d'audit en réponse à l'évaluation des risques d'anomalies significatives au niveau des assertions

Nature, calendrier et étendue des procédures d'audit complémentaires (Voir par. 6)

- A4. L'évaluation que fait l'auditeur des risques d'anomalies significatives identifiés au niveau des assertions lui fournit une base pour définir la stratégie appropriée à adopter pour la conception et la mise en œuvre des procédures d'audit complémentaires. Par exemple, l'auditeur peut déterminer :
- (a) que seuls des tests de procédures peuvent constituer une réponse efficace à son évaluation du risque d'anomalies significatives pour une assertion donnée ;
 - (b) que la mise en œuvre de contrôles de substance seulement est appropriée pour des assertions données et, de ce fait, ne pas tenir compte de l'efficacité des contrôles dans son évaluation du risque ~~concerné d'anomalies significatives~~. Cela peut être le cas lorsque, ~~du fait que les procédures d'évaluation des risques qu'il a mises en œuvre ne lui ont permis d'identifier aucun contrôle efficace pertinent pour cette assertion, ou du fait qu'il serait inefficace de tester les contrôles, l'auditeur n'a pas l'intention de s'appuyer sur l'auditeur n'a pas identifié de risque pour lequel des contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés et donc qu'il n'est pas tenu de tester l'efficacité du fonctionnement des contrôles. Ainsi, il se peut que l'auditeur ne prévoie pas de tester l'efficacité du fonctionnement des contrôles pour déterminer la nature, le calendrier et l'étendue des contrôles de substance à réaliser ;~~
 - (c) qu'une stratégie mixte associant tests de procédures et contrôles de substance constitue une stratégie efficace.

L'auditeur n'est pas tenu de concevoir ni de mettre en œuvre des procédures d'audit complémentaires à l'égard d'un risque d'anomalies significatives évalué qui se situe à un niveau suffisamment faible. Néanmoins, ainsi que l'exige le paragraphe 18, indépendamment de la stratégie retenue et de son évaluation des risques d'anomalies significatives, l'auditeur conçoit et met en œuvre des contrôles de substance pour chaque catégorie d'opérations significative, solde de compte significatif et information fournie à fournir significative, dès lors qu'ils sont significatifs.

- A5. La nature d'une procédure d'audit a trait à son objectif (tests de procédures ou contrôles de substance) et à son type (inspection, observation physique, demande d'informations, confirmation,

contrôle arithmétique, réexécution ou procédure analytique). La nature des procédures d'audit est de la plus haute importance dans l'élaboration d'une réponse à l'évaluation des risques.

- A6. Le calendrier d'une procédure d'audit a trait au moment de sa mise en œuvre, ou à la période ou à la date à laquelle se rapportent les éléments probants.
- A7. L'étendue d'une procédure d'audit a trait à l'aspect quantitatif, par exemple la taille d'un échantillon ou le nombre d'observations physiques concernant ~~une activité de contrôle~~.
- A8. Le fait de concevoir et de mettre en œuvre des procédures d'audit complémentaires dont la nature, le calendrier et l'étendue sont fonction de l'évaluation des risques d'anomalies significatives au niveau des assertions permet d'établir un lien clair entre les procédures d'audit complémentaires de l'auditeur et l'évaluation des risques.

Réponse à l'évaluation des risques au niveau des assertions (Voir par. 7 (a))

Nature

- A9. La norme ISA 315 (révisée en 2019) requiert que l'auditeur évalue le risque inhérent et le risque lié au contrôle interne aux fins de son évaluation des risques d'anomalies significatives au niveau des assertions. Pour évaluer le risque inhérent, l'auditeur détermine la probabilité et l'ampleur des anomalies en se demandant comment, et dans quelle mesure, les facteurs de risque inhérent ont une incidence sur la possibilité que les assertions pertinentes comportent des anomalies¹⁰⁴. L'évaluation des risques faite par l'auditeur ainsi que les raisons qui la sous-tendent peuvent ~~peut~~ influencer tant sur les types de procédures d'audit à mettre en œuvre que sur leur association. Par exemple, lorsqu'il évalue le risque à un niveau élevé, l'auditeur peut se faire confirmer l'exhaustivité des clauses d'un contrat par l'autre partie au contrat, en plus d'inspecter lui-même le document. Par ailleurs, certaines procédures d'audit peuvent convenir davantage à certaines assertions qu'à d'autres. Ainsi, dans le cas des produits, des tests de procédures peuvent représenter la réponse la plus adaptée à l'évaluation d'un risque d'anomalies significatives concernant l'assertion sur l'exhaustivité, tandis que des contrôles de substance peuvent être la meilleure réponse à l'évaluation d'un risque d'anomalies significatives concernant l'assertion sur la réalité.
- A10. Les raisons qui ont conduit l'auditeur à évaluer un risque comme il l'a fait sont pertinentes pour la détermination de la nature des procédures d'audit. Par exemple, si un niveau de risque est considéré comme faible en raison des caractéristiques particulières d'une catégorie donnée d'opérations, indépendamment des contrôles les concernant, l'auditeur peut décider que la mise en œuvre de procédures analytiques de substance est suffisante pour l'obtention d'éléments probants suffisants et appropriés. En revanche, si le niveau de risque est considéré comme faible ~~en raison de certains~~ parce que l'auditeur prévoit de tester l'efficacité du fonctionnement des contrôles internes, et que l'auditeur qu'il a l'intention de concevoir des contrôles de substance sur la base de cette évaluation, il exécute alors des tests de ces contrôles, comme le requiert le paragraphe 8 a). Ce peut être le cas, par exemple, pour un flux d'opérations dotées de caractéristiques raisonnablement homogènes,

¹⁰⁴ Norme ISA 315 (révisée en 2019), paragraphes 31 et 34.

dénuées de complexité et qui sont systématiquement traitées et contrôlées par le système informatique de l'entité.

Calendrier

- A11. L'auditeur peut mettre en œuvre des tests de procédures ou des contrôles de substance à une date intermédiaire ou à la fin de la période. Plus le risque d'anomalies significatives est élevé, plus il est probable que l'auditeur décidera qu'il est plus efficace de mettre en œuvre des contrôles de substance à la fin de la période ou à une date proche de celle-ci plutôt qu'à une date antérieure, ou de mettre en œuvre des procédures d'audit non annoncées ou inopinées (par exemple, mettre en œuvre des procédures d'audit dans des établissements sélectionnés sans annonce préalable). De telles décisions sont particulièrement pertinentes lors de la prise en considération des réponses aux risques de fraude. Ainsi, lorsque des risques d'anomalies intentionnelles ou de manipulations ont été identifiés, il peut arriver que l'auditeur conclue que des procédures destinées à étendre jusqu'à la fin de la période les conclusions de ses travaux réalisés à une date intermédiaire ne seraient pas efficaces.
- A12. Inversement, la mise en œuvre de procédures d'audit avant la fin de la période peut aider l'auditeur à identifier les problèmes importants à un stade préliminaire de l'audit et donc à les résoudre avec l'assistance de la direction ou à mettre au point une stratégie d'audit efficace en réponse à ces problèmes.
- A13. Par ailleurs, certaines procédures d'audit ne sauraient être mises en œuvre avant la date de clôture, par exemple :
- la vérification de la concordance ou le rapprochement des données communiquées dans les états financiers, y compris des informations fournies, avec les documents comptables sous-jacents, que celles-ci proviennent ou non du grand livre et des journaux auxiliaires ;
 - le contrôle des ajustements effectués lors de la préparation des états financiers ;
 - les procédures répondant au risque que, à la fin de la période, l'entité ait pu conclure des contrats de vente irréguliers ou que des opérations non finalisées aient été comptabilisées.
- A14. Lorsque l'auditeur s'interroge sur le moment de mettre en œuvre des procédures d'audit, il tient également compte des facteurs suivants :
- l'environnement de contrôle ;
 - le moment où les informations pertinentes sont disponibles (par exemple, certains fichiers informatiques peuvent être ultérieurement écrasés ou l'observation physique de certaines procédures peut n'être possible qu'à des moments particuliers) ;
 - la nature du risque (par exemple, s'il y a un risque de surévaluation des produits pour satisfaire aux attentes concernant les bénéficiaires, par la création ultérieure de faux contrats de vente, l'auditeur souhaitera peut-être examiner les contrats en cours à la fin de la période) ;
 - la période ou la date à laquelle se rapportent les éléments probants ;
 - le moment de la préparation des états financiers, notamment lorsque des informations sont fournies pour donner des explications supplémentaires sur les montants inscrits dans l'état de

la situation financière, l'état du résultat global, l'état des variations des capitaux propres et le tableau des flux de trésorerie.

Étendue

- A15. Pour juger de l'étendue à donner à une procédure d'audit, l'auditeur tient compte du seuil de signification, de son évaluation du risque et du niveau d'assurance qu'il souhaite obtenir. Lorsque plusieurs procédures sont exécutées en association en vue d'un seul objectif, l'auditeur s'interroge séparément sur l'étendue de chaque procédure. En général, l'étendue des procédures d'audit sera d'autant plus grande que le risque d'anomalies significatives est élevé. Par exemple, pour répondre à l'évaluation du risque d'anomalies significatives résultant de fraudes, il peut être approprié d'augmenter la taille des échantillons ou de mettre en œuvre des procédures analytiques de substance à un niveau de détail plus poussé. Cela dit, augmenter l'étendue d'une procédure d'audit n'est efficace que si la procédure d'audit est pertinente par rapport au risque considéré.
- A16. L'utilisation de techniques d'audit assistées par ordinateur peut permettre des tests de plus grande ampleur des opérations automatisées et des fichiers comptables, ce qui peut être utile lorsque l'auditeur décide de modifier l'étendue des tests, par exemple en réponse aux risques d'anomalies significatives résultant de fraudes. Ces techniques peuvent être utilisées pour sélectionner des échantillons d'opérations dans des fichiers électroniques clés, trier des opérations dotées de certaines caractéristiques particulières ou tester une population entière plutôt qu'un échantillon.

Considérations propres aux entités du secteur public

- A17. Lorsque l'audit porte sur une entité du secteur public, la détermination de la nature, du calendrier et de l'étendue des procédures d'audit complémentaires peut être influencée par le mandat d'audit et par l'existence éventuelle d'diligences particulières applicables à la mission.

Considérations propres aux petites entités

- A18. Dans le cas des très petites entités, il peut arriver que les ~~contrôles-mesures de contrôle~~ contrôles identifiables par l'auditeur soient rares ou que la mesure dans laquelle leur existence ou leur fonctionnement ont été documentés par l'entité soit limitée. En pareille situation, il se peut qu'il soit plus efficace pour l'auditeur de privilégier les contrôles de substance dans le choix de ses procédures d'audit complémentaires. Dans de rares cas, par ailleurs, l'absence ~~d-mesures de contrôle~~ de contrôles ou ~~d'autres éléments de composantes du système de~~ contrôle interne peut rendre impossible l'obtention d'éléments probants suffisants et appropriés.

Risque élevé (Voir par. 7 (b))

- A19. Lorsque, par suite de son évaluation, l'auditeur considère que le risque est élevé et qu'il cherche à recueillir des éléments probants plus convaincants, il peut en recueillir un plus grand nombre ou en recueillir qui soient plus pertinents et plus fiables, par exemple en accordant plus d'importance à des

éléments émanant de tiers ou à des éléments corroborants provenant de plusieurs sources indépendantes.

Test des contrôles

Conception et mise en œuvre des tests de procédures (Voir par. 8)

- A20. Seuls sont soumis à des tests les contrôles que l'auditeur juge correctement conçus pour prévenir, ou détecter et corriger, une anomalie significative concernant une assertion pertinente, et qu'il a prévu de tester. Lorsque des contrôles substantiellement différents ont été appliqués à divers moments de la période audité, chacun de ces contrôles est pris en considération séparément.
- A21. Il existe une différence entre tester l'efficacité du fonctionnement des contrôles, d'une part, et comprendre et évaluer leur conception et leur mise en œuvre, d'autre part. Cependant, les mêmes types de procédures sont appliqués dans les deux cas. L'auditeur peut donc juger efficient de procéder simultanément au test de l'efficacité du fonctionnement des contrôles, ainsi qu'à l'évaluation de leur conception et à la vérification de leur mise en œuvre.
- A22. En outre, il peut arriver que, sans avoir été expressément conçues pour tester les contrôles, certaines procédures d'évaluation des risques procurent des éléments probants sur l'efficacité de leur fonctionnement et, partant, servent de tests de procédures. Par exemple, dans le cadre de ses procédures d'évaluation des risques, l'auditeur peut avoir :
- demandé à la direction des informations sur l'utilisation qu'elle fait des budgets ;
 - observé le processus suivi par la direction pour comparer les charges mensuelles budgétées et les charges réelles ;
 - examiné les rapports d'analyse des écarts entre les montants budgétés et les montants réels.

Non seulement ces procédures renseignent l'auditeur sur la conception des politiques budgétaires de l'entité et sur la réalité de leur application, mais elles peuvent aussi lui fournir des éléments probants sur l'efficacité du fonctionnement des politiques budgétaires de l'entité pour ce qui concerne la prévention ou la détection des anomalies significatives dans le classement des charges.

- A23. De plus, l'auditeur peut concevoir un test des contrôles à mettre en œuvre conjointement avec un test de détail portant sur la même opération. Bien que le test des contrôles n'ait pas le même objectif que le test de détail, la simultanéité d'exécution est possible, et l'on peut alors parler de test à double objectif. Par exemple, l'auditeur peut concevoir un test et en évaluer les résultats dans le cadre de l'examen d'une facture pour, d'une part, déterminer si elle a été approuvée et, d'autre part, obtenir un élément probant corroborant une opération. Pour concevoir un test à double objectif comme pour en évaluer les résultats, l'auditeur considère chaque objectif séparément.
- A24. Dans certaines situations, l'auditeur peut conclure à l'impossibilité de concevoir des contrôles de substance qui soient assez efficaces pour fournir à eux seuls des éléments probants suffisants et appropriés au niveau des assertions¹⁰⁵. Ce peut être le cas lorsqu'une entité dont le fonctionnement

¹⁰⁵ Norme ISA 315 (révisée en 2019), paragraphe 3330.

est informatisé ne produit ou ne conserve aucune documentation sur ses opérations, si ce n'est dans le système informatique. En pareil cas, l'e paragraphe 8 (b) requiert que l'auditeur ~~soumette~~ teste les contrôles ~~concernés à des tests qui concernent les risques pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés.~~

Éléments probants et intention de s'appuyer sur les contrôles (Voir par. 9)

A25. L'auditeur peut chercher à obtenir un niveau d'assurance plus élevé quant à l'efficacité du fonctionnement des contrôles lorsque sa stratégie consiste principalement à mettre en œuvre des tests de procédures, surtout si l'obtention d'éléments probants suffisants et appropriés n'est pas possible ou faisable en pratique au moyen de contrôles de substance seulement.

Nature et étendue des tests de procédures

Autres procédures d'audit associées aux demandes d'informations (Voir par. 10 (a))

A26. Les demandes d'informations ne permettent pas à elles seules de tester l'efficacité du fonctionnement des contrôles. En conséquence, d'autres procédures sont mises en œuvre en association avec elles. À cet égard, l'association de demandes d'informations et de procédures d'inspection ou de réexécution peut fournir un niveau plus élevé d'assurance que l'association de demandes d'informations et de procédures d'observation physique, car celles-ci ne valent que pour le moment où elles sont réalisées.

A27. Le type de procédure requis pour recueillir des éléments probants quant à l'efficacité du fonctionnement d'un contrôle est fonction de la nature de celui-ci. Par exemple, lorsque l'efficacité du fonctionnement est documentée, l'auditeur peut décider d'inspecter les documents pour recueillir des éléments probants attestant cette efficacité. Il arrive en revanche que certains contrôles ne fassent l'objet d'aucune documentation, du moins pertinente. Par exemple, il se peut que ne soit consigné nulle part le fonctionnement de certains aspects de l'environnement de contrôle, tels que la délégation des pouvoirs et des responsabilités, ou de certains types ~~de contrôles d' mesures de contrôle de contrôles, telles que celles qui sont exécutées par un ordinateur~~ tels que les contrôles automatisés. En pareille situation, les éléments probants portant sur l'efficacité du fonctionnement peuvent être recueillis par des demandes d'informations en association avec d'autres procédures d'audit, comme l'observation ou les techniques d'audit assistées par ordinateur.

Étendue des tests de procédures

A28. Lorsque des éléments probants plus convaincants sont nécessaires pour pouvoir attester l'efficacité d'un contrôle, il peut être approprié d'augmenter l'étendue des tests sur ce contrôle. Pour déterminer l'étendue des tests de procédures, outre la mesure dans laquelle il compte s'appuyer sur les contrôles, l'auditeur peut tenir compte des éléments suivants :

- la fréquence de l'exécution du contrôle par l'entité pendant la période ;
- la durée, au cours de la période auditée, pour laquelle il s'appuie sur l'efficacité du fonctionnement du contrôle ;

- le taux d'écart attendu par rapport au contrôle ;
- la pertinence et la fiabilité des éléments probants à recueillir concernant l'efficacité du fonctionnement du contrôle au niveau d'une assertion ;
- la mesure dans laquelle des éléments probants sont recueillis en testant d'autres contrôles relatifs à l'assertion.

La norme ISA 530¹⁰⁶ contient des indications complémentaires sur l'étendue à donner aux tests.

A29. En raison de l'uniformité inhérente au traitement informatique, il se peut qu'il ne soit pas nécessaire d'augmenter l'étendue des tests sur un contrôle automatisé. On peut s'attendre au fonctionnement uniforme d'un contrôle automatisé tant que ~~le programme~~ l'application informatique (y compris les tables, les fichiers et les autres données permanentes utilisés par ~~le programme~~ celle-ci) n'est pas modifiée. Une fois que l'auditeur a déterminé qu'un contrôle automatisé fonctionne comme prévu (ce qu'il peut faire lors de la mise en œuvre initiale du contrôle ou à toute autre date), il peut envisager d'effectuer des tests pour vérifier que le contrôle continue de fonctionner efficacement. L'auditeur peut ~~Les tests peuvent~~ notamment tester les contrôles généraux informatiques portant sur l'application informatique, consister à vérifier que :

- ~~des modifications ne sont pas apportées au programme sans être soumises à des contrôles appropriés ;~~
- ~~la version autorisée du programme est utilisée pour le traitement des opérations ;~~
- ~~d'autres contrôles généraux pertinents sont efficaces.~~

~~Ces tests peuvent aussi consister à vérifier que les programmes n'ont pas subi de modifications, par exemple dans le cas où l'entité utilise des logiciels d'application prêts à l'emploi sans les modifier ni les mettre à jour. Ainsi, l'auditeur peut inspecter les archives du service chargé de la sécurité informatique pour obtenir des éléments probants montrant qu'aucun accès non autorisé n'a eu lieu pendant la période considérée.~~

A29a. De même, l'auditeur peut mettre en œuvre des tests de procédures qui permettent de répondre aux risques d'anomalies significatives concernant l'intégrité des données de l'entité ou l'exhaustivité et l'exactitude des rapports générés par le système de l'entité, ou des contrôles qui concernent les risques d'anomalies significatives pour lesquels les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés. Ces tests de procédures peuvent entre autres porter sur des contrôles généraux informatiques et tenir compte des éléments mentionnés au paragraphe 10 a). Lorsque c'est le cas, l'auditeur peut ne pas avoir à mettre en œuvre d'autres tests pour recueillir des éléments probants sur ces éléments.

A29b. Lorsqu'il détermine qu'un contrôle général informatique est déficient, l'auditeur peut prendre en considération la nature des risques connexes provenant du recours à l'informatique – risques qu'il a identifiés en application de la norme ISA 315 (révisée en 2019)¹⁰⁷ –, afin de disposer d'une base pour la conception de procédures d'audit supplémentaires permettant de répondre à son évaluation du risque d'anomalies significatives. Ces procédures supplémentaires peuvent notamment servir à déterminer :

¹⁰⁶ Norme ISA 530, *Sondages en audit*.

¹⁰⁷ Norme ISA 315 (révisée en 2019), sous-par. 26 (c)(i).

- si les risques connexes provenant du recours à l'informatique se sont concrétisés. Par exemple, si certains utilisateurs disposent d'un accès non autorisé à une application informatique, mais qu'ils ne peuvent ni accéder à l'historique des accès du système ni le modifier, l'auditeur peut inspecter cet historique afin de recueillir des éléments probants attestant que ces utilisateurs n'ont pas accédé à l'application informatique au cours de la période ;
- s'il y a des contrôles de remplacement, des contrôles redondants ou d'autres contrôles visant à répondre aux risques connexes provenant du recours à l'informatique. Lorsqu'il y en a, l'auditeur peut identifier ces contrôles (s'il ne l'a pas déjà fait), puis en évaluer la conception, déterminer s'ils ont été mis en œuvre et en tester l'efficacité du fonctionnement. Par exemple, s'agissant de la déficience d'un contrôle général informatique lié aux accès, il se peut que l'entité ait prévu, en guise de contrôle de remplacement, que la direction du service informatique examine en temps opportun des rapports sur les accès des utilisateurs finaux. Il peut y avoir des circonstances où des contrôles des applications permettent de répondre aux risques provenant du recours à l'informatique lorsque, par exemple, les informations potentiellement affectée par la déficience du contrôle général informatique peuvent faire l'objet d'un rapprochement avec des informations provenant de sources externes (par exemple, un relevé bancaire) ou de sources internes qui ne sont pas touchées par cette déficience (par exemple, une autre application informatique ou une autre source de données).

Tests de procédures indirects (Voir par. 10 (b))

~~A30.~~ Dans certaines situations, il peut être nécessaire de recueillir des éléments probants attestant l'efficacité du fonctionnement de contrôles indirects (par exemple, de contrôles généraux informatiques). Comme il est expliqué aux paragraphes A29–A29b, il se peut que des contrôles généraux informatiques aient été identifiés, en application de la norme ISA 315 (révisée en 2019), du fait qu'ils assurent l'efficacité du fonctionnement de contrôles automatisés ou le maintien de l'intégrité des informations qui sont utilisées dans le cadre du processus d'information financière de l'entité, y compris les rapports générés par le système. L'exigence énoncée au paragraphe 10 (b) évoque la possibilité que l'auditeur ait déjà testé certains contrôles indirects en ce qui concerne les éléments mentionnés au paragraphe 10 (a). Par exemple, lorsque l'auditeur décide de tester la revue faite par un utilisateur des relevés des écarts correspondant à des dépassements de la limite de crédit autorisée par client, cette revue de l'utilisateur et le suivi qui en découle constituent le contrôle directement pertinent pour l'auditeur. Les contrôles portant sur l'exactitude des informations contenues dans les relevés (par exemple, les contrôles généraux auxquels sont soumis les systèmes informatiques) sont qualifiés de contrôles « indirects ».

~~A31.~~ En raison de l'uniformité inhérente au traitement informatique, les éléments probants concernant la mise en place d'un contrôle d'application automatisé, considérés conjointement avec les éléments probants obtenus sur l'efficacité du fonctionnement des contrôles généraux de l'entité (en particulier,

~~les contrôles sur les modifications de programmes), peuvent aussi fournir des éléments probants substantiels quant à l'efficacité du fonctionnement du contrôle d'application en question.~~

Calendrier des tests de procédures

Période pour laquelle l'auditeur a l'intention de s'appuyer sur les contrôles (Voir par. 11)

A32. Il peut arriver que des éléments probants qui se rapportent uniquement à un moment précis soient suffisants pour satisfaire à l'objectif de l'auditeur, par exemple dans le cas d'un test des contrôles portant sur la prise d'inventaire physique de fin de période. Si, en revanche, l'auditeur entend s'appuyer sur un contrôle pour l'ensemble d'une période donnée, il convient qu'il mette en œuvre des tests lui permettant de recueillir des éléments probants attestant l'efficacité du fonctionnement du contrôle à des moments pertinents pendant cette période. Ces tests de procédures peuvent notamment porter sur le des contrôles qui font partie du processus de suivi du système de contrôle interne par que fait l'entité de ses propres contrôles.

Utilisation d'éléments probants recueillis au cours d'une période intermédiaire (Voir par. 12 (b))

A33. Parmi les facteurs pertinents pour la détermination des éléments probants additionnels à obtenir sur le fonctionnement des contrôles en œuvre pendant la période restant à couvrir après une période intermédiaire, il y a les suivants :

- l'importance des risques d'anomalies significatives au niveau des assertions, selon l'évaluation de l'auditeur ;
- les contrôles spécifiques qui ont été testés pendant la période intermédiaire, et les changements importants qu'ils ont subis depuis, y compris les changements intervenus dans le système d'information, les processus ou le personnel ;
- la mesure dans laquelle l'auditeur a recueilli des éléments probants quant à l'efficacité du fonctionnement de ces contrôles ;
- la durée de la période restant à couvrir ;
- la mesure dans laquelle l'auditeur a l'intention de réduire les contrôles de substance complémentaires en raison de la confiance qu'il accorde aux contrôles ;
- l'environnement de contrôle.

A34. Pour obtenir ces éléments probants additionnels, l'auditeur peut par exemple étendre les tests de procédures sur la période restant à couvrir ou tester le suivi que fait l'entité sur ses propres contrôles.

Utilisation d'éléments probants recueillis au cours des audits précédents (Voir par. 13)

A35. Dans certains cas, les éléments probants recueillis au cours des audits précédents peuvent de nouveau servir d'éléments probants lorsque l'auditeur met en œuvre des procédures d'audit confirmant qu'ils sont toujours pertinents et fiables. Par exemple, lors d'un audit précédent, l'auditeur peut avoir déterminé qu'un contrôle automatisé fonctionnait comme prévu. Il peut alors recueillir des éléments probants qui lui permettent de déterminer si le contrôle en question a fait l'objet de modifications affectant l'efficacité continue de son fonctionnement, par exemple par des demandes d'informations auprès de la direction et par l'inspection des journaux des interventions indiquant les

contrôles qui ont été modifiés. La prise en considération des éléments probants portant sur ces modifications peut entraîner soit une augmentation, soit une diminution, des éléments probants à recueillir pendant la période en cours relativement à l'efficacité du fonctionnement de ces contrôles.

Contrôles modifiés depuis les audits précédents (Voir par. 14 (a))

A36. Il peut arriver que des changements réduisent la pertinence et la fiabilité des éléments probants recueillis lors des audits précédents au point de leur faire perdre toute utilité pour l'audit en cours. Par exemple, s'il est peu probable que des modifications apportées à un système pour lui faire produire un nouveau type de rapport utilisable par l'entité réduisent la pertinence des éléments probants recueillis lors d'un audit précédent, en revanche, une modification du système qui implique que des données soient désormais cumulées ou calculées différemment en réduit la pertinence.

Contrôles inchangés depuis les audits précédents (Voir par. 14 (b))

A37. La décision de l'auditeur de s'appuyer ou non sur des éléments probants recueillis lors d'audits précédents pour des contrôles qui :

- (a) d'une part, n'ont subi aucun changement depuis les derniers tests auxquels ils ont été soumis,
- (b) d'autre part, n'ont pas pour effet d'atténuer un risque important,

relève du jugement professionnel. Par ailleurs, la durée du délai que l'auditeur peut laisser s'écouler avant de retester ces contrôles relève également du jugement professionnel, sous réserve que chaque contrôle soit testé au moins une fois tous les trois audits, ainsi que l'exige le paragraphe 14 (b).

A38. En général, plus le risque d'anomalies significatives est élevé, ou plus l'auditeur s'appuie sur les contrôles, plus il est probable que le délai avant un nouveau test sera court, à supposer que le contrôle ne soit pas soumis à un test lors de chaque audit. Les facteurs susceptibles d'avoir pour effet de réduire ce délai ou de conduire l'auditeur à ne pas s'appuyer du tout sur les éléments probants recueillis lors des audits précédents sont notamment :

- un environnement de contrôle déficient ;
- ~~un suivi déficient des contrôles~~ une déficience du processus de suivi du système de contrôle interne par l'entité ;
- l'importance de l'intervention humaine dans le fonctionnement des contrôles ~~concernés~~ ;
- l'importance de l'incidence des changements de personnel sur le fonctionnement des contrôles ;
- les changements de circonstances qui appellent une modification des contrôles ;
- des contrôles informatiques généraux qui sont déficients.

A39. Lorsqu'il existe un certain nombre de contrôles pour lesquels l'auditeur a l'intention de s'appuyer sur des éléments probants recueillis lors des audits précédents, le fait de tester certains de ces contrôles au cours de chaque audit fournit à l'auditeur des informations confirmant l'efficacité continue de

l'environnement de contrôle. Cela aide l'auditeur à décider s'il convient ou non de s'appuyer sur des éléments probants recueillis lors des audits précédents.

Évaluation de l'efficacité du fonctionnement des contrôles (Voir par. 16–17)

- A40. La détection d'une anomalie significative par les procédures de l'auditeur constitue une indication forte d'une déficience importante du contrôle interne.
- A41. Le concept de l'efficacité du fonctionnement des contrôles n'exclut pas la possibilité d'écarts dans la façon dont les contrôles sont appliqués par l'entité. Ces écarts par rapport aux contrôles prescrits peuvent être causés par des facteurs tels que des changements dans le personnel clé, des fluctuations saisonnières importantes du volume d'opérations ou des erreurs humaines. Le taux d'écart relevé, et plus précisément la mesure dans laquelle il excède le taux d'écart attendu, peut indiquer qu'il n'y a pas lieu de penser que le contrôle concerné soit suffisant pour ramener le risque au niveau des assertions à celui évalué par l'auditeur.

Contrôles de substance (Voir par. 6, 18)

A42. Le paragraphe 18 requiert de l'auditeur qu'il conçoive et mette en œuvre des contrôles de substance pour chaque catégorie d'opérations significative, chaque solde de compte significatif et chaque information fournie à fournir significative, ~~dès lors qu'ils sont significatifs, et ce, indépendamment de son évaluation du risque d'anomalies significatives.~~ En ce qui concerne les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes, il se peut que des contrôles de substance aient déjà été mis en œuvre, car le paragraphe 6 requiert de l'auditeur qu'il conçoive et mette en œuvre des procédures d'audit complémentaires adaptées à son évaluation des risques d'anomalies significatives au niveau des assertions. Des contrôles de substance doivent donc être conçus et mis en œuvre conformément au paragraphe 18 :

- lorsqu'il n'y a pas de contrôles de substance parmi les procédures d'audit complémentaires conçues et mises en œuvre conformément au paragraphe 6 à l'égard des flux d'opérations importants, des soldes de comptes importants et des informations à fournir importantes ;
- pour chaque flux d'opérations, chaque solde de compte et chaque information à fournir qui ne constitue pas un flux d'opérations important, un solde de compte important ou une information à fournir importante, mais qui a été identifié comme étant significatif en application de la norme ISA 315 (révisée en 2019)¹⁰⁸.
- Cette exigence reflète le fait : a) que l'évaluation du risque par l'auditeur est affaire de jugement et ne permet pas nécessairement d'identifier tous les risques d'anomalies significatives, et b) qu'il existe des limites inhérentes aux contrôles interne, notamment la possibilité de ~~son leur~~ contournement par la direction.

A42a. Il n'est pas obligatoire de tester toutes les assertions relatives à un flux d'opérations significative, à un solde de compte significatif ou à une information à fournir significative. Lors de la conception des contrôles de substance à mettre en œuvre, la prise en compte des assertions pour lesquelles il y a une possibilité

¹⁰⁸ Norme ISA 315 (révisée), paragraphe 36.

raisonnable qu'une anomalie, si elle venait à se produire, soit significative, peut aider l'auditeur à déterminer la nature, le calendrier et l'étendue qui conviennent pour les procédures à mettre en œuvre.

Nature et étendue des contrôles de substance

A43. Selon le cas, l'auditeur peut déterminer :

- que la mise en œuvre de procédures analytiques de substance sera suffisante à elle seule pour ramener le risque d'audit à un niveau suffisamment faible. C'est le cas, par exemple, lorsque l'évaluation du risque faite par l'auditeur est étayée par des éléments probants recueillis au moyen de tests de procédures ;
- que seuls des tests de détail conviennent ;
- que la meilleure réponse à l'évaluation du risque consiste à associer des procédures analytiques de substance à des tests de détail.

A44. Les procédures analytiques de substance sont généralement plus adaptées à des volumes importants d'opérations qui ont tendance à devenir prévisibles au fil du temps. La norme ISA 520¹⁰⁹ définit des diligences et fournit des indications concernant la mise en œuvre de procédures analytiques au cours d'un audit.

A45. La conception des tests de détail est influencée par ~~la nature~~ l'évaluation du risque ~~et celle ou par la nature~~ de l'assertion. Par exemple, les tests de détail relatifs aux assertions sur l'existence ou sur la réalité peuvent impliquer de sélectionner des éléments dans un poste des états financiers et de recueillir des éléments probants les concernant. En revanche, les tests de détail relatifs à l'assertion sur l'exhaustivité peuvent consister à sélectionner des éléments que devrait normalement contenir un poste des états financiers et à vérifier si ces éléments s'y trouvent effectivement.

A46. Étant donné que l'évaluation du risque d'anomalies significatives tient compte ~~des contrôles du contrôle interne que l'auditeur prévoit de tester~~, il se peut qu'il faille augmenter l'étendue des contrôles de substance lorsque les résultats des tests de procédures ne sont pas satisfaisants. Cela dit, augmenter ainsi l'étendue d'une procédure d'audit n'est approprié que si cette dernière est pertinente par rapport au risque considéré.

A47. Lors de la conception des tests de détail, l'étendue des tests est souvent envisagée en termes de taille de l'échantillon. Toutefois, d'autres considérations sont également pertinentes ; on peut notamment se demander s'il ne serait pas plus efficace d'avoir recours à un autre mode de sélection d'éléments à des fins de tests. Voir la norme ISA 500¹¹⁰.

Détermination de la nécessité de mettre en œuvre des procédures de confirmation externe (Voir par. 19)

A48. Les procédures de confirmation externe sont souvent pertinentes pour vérifier les assertions relatives à des soldes de comptes et leurs composantes, mais il n'y a pas lieu de limiter leur utilisation à ces seuls éléments. Par exemple, l'auditeur peut demander une confirmation externe des termes d'accords, de contrats ou d'opérations que l'entité a conclus avec des tiers. Les confirmations

¹⁰⁹ Norme ISA 520, *Procédures analytiques*.

¹¹⁰ Norme ISA 500, *Éléments probants*, paragraphe 10

externes peuvent également être utilisées pour recueillir des éléments probants quant à l'absence de certaines conditions. Par exemple, une demande peut viser spécifiquement à faire confirmer l'absence d'un « accord parallèle » qui pourrait être pertinent en ce qui concerne l'assertion relative à la séparation des périodes pour la comptabilisation des produits de l'entité. Les procédures de confirmation externe peuvent aussi fournir des éléments probants pertinents, dans le cadre des réponses de l'auditeur à son évaluation des risques d'anomalies significatives, à l'égard par exemple :

- des soldes de comptes bancaires et d'autres informations concernant les relations avec les banques ;
- des soldes et conditions des comptes clients ;
- des stocks détenus par des tiers soit en entrepôt de douane en attente de traitement, soit en consignation ;
- des titres de propriété déposés en garde ou en nantissement auprès d'avocats ou d'établissements financiers ;
- des valeurs mobilières sous la garde de tiers, ou achetées de courtiers en valeurs mobilières mais non encore livrées à la date de clôture ;
- des montants dus à des prêteurs, y compris les modalités de remboursement pertinentes et les clauses restrictives ;
- des soldes et conditions des comptes fournisseurs.

A49. Les confirmations externes peuvent fournir des éléments probants pertinents à l'égard de certaines assertions, mais des éléments probants moins pertinents dans le cas d'autres assertions. Par exemple, elles procurent des éléments probants moins pertinents en ce qui concerne la recouvrabilité des soldes de comptes clients qu'en ce qui concerne leur existence.

A50. L'auditeur peut déterminer que les procédures de confirmation externe mises en œuvre dans un but donné procurent l'occasion de recueillir des éléments probants sur d'autres questions. Par exemple, les demandes de confirmation portant sur des soldes de comptes bancaires comportent souvent des demandes d'informations pertinentes pour d'autres assertions contenues dans les états financiers. De telles considérations peuvent influencer sur la décision de l'auditeur de mettre en œuvre ou non des procédures de confirmation externe.

A51. Voici d'autres facteurs qui peuvent aider l'auditeur à déterminer si des procédures de confirmation externe doivent être mises en œuvre en tant que contrôles de substance :

- la connaissance qu'a le tiers de l'objet de la demande de confirmation – il se peut que les réponses soient plus fiables si la personne qui répond au nom du tiers a une connaissance suffisante de l'information à confirmer ;
- la capacité et la volonté de répondre du tiers visé. Il se peut par exemple que le tiers :
 - refuse d'assumer la responsabilité liée à la réponse à une demande de confirmation,
 - considère que le processus de réponse est trop coûteux ou prend trop de temps,
 - craigne de voir sa responsabilité éventuellement engagée du fait de sa réponse,
 - comptabilise les opérations dans des monnaies différentes,

- exerce ses activités dans un environnement où le fait de répondre à des demandes de confirmation ne constitue pas un aspect important des activités courantes.

En pareil cas, il se peut que les tiers ne répondent pas, répondent à la légère ou tentent de limiter la confiance à accorder à la réponse ;

- l'objectivité du tiers – si le tiers est une partie liée à l'entité, il se peut que les réponses aux demandes de confirmation soient moins fiables.

Contrôles de substance liés au processus de finalisation des états financiers (Voir par. 20 (b))

A52. La nature ainsi que l'étendue de la vérification, par l'auditeur, des écritures comptables et des autres ajustements sont fonction de la nature et de la complexité du processus d'information financière de l'entité et des risques d'anomalies significatives y afférents.

Contrôles de substance en réponse aux risques importants (Voir par. 21)

A53. Le paragraphe 21 de la présente norme ISA requiert de l'auditeur qu'il mette en œuvre des contrôles de substance répondant spécifiquement aux risques qu'il a définis comme étant importants. Les éléments probants recueillis sous forme de confirmations externes que l'auditeur reçoit directement de tiers compétents peuvent contribuer à l'obtention des éléments probants caractérisés par le haut niveau de fiabilité dont il a besoin pour répondre aux risques importants d'anomalies significatives, que celles-ci résultent de fraudes ou d'erreurs. Par exemple, si l'auditeur constate que la direction subit des pressions pour atteindre les résultats attendus, il peut y avoir un risque qu'elle gonfle le chiffre d'affaires en comptabilisant indûment des produits dont la comptabilisation n'est pas permise en raison des modalités des contrats de vente ou en facturant des ventes avant l'expédition. En pareil cas, l'auditeur peut, par exemple, concevoir des procédures de confirmation externe pour faire confirmer non seulement les soldes de compte, mais aussi les termes des contrats de vente, y compris la date, les conditions de reprise éventuelle de la marchandise et les modalités de livraison. De plus, il peut juger efficace de compléter ces procédures de confirmation externe par des demandes d'informations auprès du personnel non financier de l'entité afin de vérifier si les termes des contrats de vente ou les modalités de livraison n'auraient pas été modifiés.

Calendrier des contrôles de substance (Voir par. 22–23)

A54. Dans la plupart des cas, il y a peu ou pas d'éléments probants recueillis par la mise en œuvre de contrôles de substance lors d'un audit précédent qui demeurent pertinents pour la période précédente. Il existe toutefois des exceptions. Ainsi, un avis juridique obtenu lors d'un audit précédent au sujet d'une structure de titrisation qui n'a subi aucune modification depuis peut être encore pertinent pour la période en cours. Dans de tels cas, il peut être approprié d'utiliser des éléments probants recueillis par la mise en œuvre de contrôles de substance lors d'un audit précédent, pourvu que ni les éléments probants ni leur objet n'aient fondamentalement changé et que des procédures d'audit aient été mises en œuvre pour la période en cours de manière à établir que ces éléments probants n'ont rien perdu de leur pertinence.

Utilisation d'éléments probants recueillis au cours d'une période intermédiaire (Voir par. 22)

A55. Dans certains cas, l'auditeur peut juger efficace de mettre en œuvre des contrôles de substance à une date intermédiaire et d'effectuer une comparaison et un rapprochement des informations sur les soldes de clôture avec les informations correspondantes recueillies à la date intermédiaire afin :

- (a) d'identifier les montants qui paraissent inhabituels ;
- (b) de procéder à des investigations sur ces montants ;
- (c) de procéder, pour le restant de l'exercice, à des procédures analytiques de substance ou à des tests de détail.

A56. Lorsque l'auditeur met en œuvre des contrôles de substance à une date intermédiaire, sans en réaliser d'autres à une date ultérieure, il s'expose à un risque accru de ne pas détecter des anomalies pouvant exister à la fin de l'exercice. Ce risque est d'autant plus grand que la partie de l'exercice restant à couvrir est longue. Les facteurs suivants, entre autres, peuvent influencer sur la décision de mettre en œuvre ou non des contrôles de substance à une date intermédiaire :

- l'environnement de contrôle et les autres contrôles pertinents ;
- la disponibilité, à une date ultérieure, d'informations nécessaires à la mise en œuvre des procédures d'audit ;
- le but de la procédure de corroboration ;
- l'évaluation du risque d'anomalies significatives ;
- la nature de la catégorie d'opérations ou du solde de compte et les assertions sous-jacentes ;
- la possibilité, pour l'auditeur, de mettre en œuvre, pour le restant de l'exercice, des contrôles de substance appropriés ou des contrôles de substance associés à des tests de procédures, afin de réduire le risque de non-détection d'anomalies existant à la fin de l'exercice.

A57. Les facteurs suivants, entre autres, peuvent influencer sur la décision de mettre en œuvre des procédures analytiques de substance pour la période comprise entre la date intermédiaire et la fin de l'exercice :

- le caractère raisonnablement prévisible ou non des données de clôture des flux d'opérations ou des soldes de comptes concernés pour ce qui est de leur montant, de leur importance relative et des éléments qui les composent ;
- le caractère approprié ou non des procédures de l'entité pour l'analyse et l'ajustement de ces flux d'opérations ou soldes de comptes à des dates intermédiaires ainsi que de ses procédures de séparation des exercices ;
- la fourniture ou non, par le système d'information pertinent pour l'information financière, d'informations suffisantes sur les soldes de clôture et les opérations réalisées pendant le restant de l'exercice pour permettre de procéder à des investigations sur :
 - (a) les opérations ou les écritures inhabituelles importantes (y compris celles intervenues à la fin de l'exercice ou à une date qui en est proche),
 - (b) les autres causes de variations importantes, ou les variations prévues qui ne se sont pas produites,
 - (c) les changements dans la composition des flux d'opérations ou des soldes de comptes.

Anomalies détectées à une date intermédiaire (Voir par. 23)

A58. Lorsque l'auditeur conclut à la nécessité de modifier la nature, le calendrier ou l'étendue prévus des contrôles de substance couvrant le restant de l'exercice parce qu'il a détecté des anomalies inattendues à une date intermédiaire, il peut notamment étendre ou répéter à la fin de l'exercice les procédures mises en œuvre à la date intermédiaire.

Caractère adéquat de la présentation des états financiers (Voir par. 24)

A59. Évaluer le caractère approprié de la présentation, de la disposition et du contenu des états financiers consiste, par exemple, à prendre en considération la terminologie employée selon les diligences du référentiel comptable applicable, le niveau de détail fourni, le regroupement ou la ventilation des montants et les modes de détermination des montants présentés.

Évaluation du caractère suffisant et approprié des éléments probants recueillis (Voir par. 25–27)

A60. Un audit d'états financiers est un processus cumulatif et itératif. À mesure que l'auditeur met en œuvre des procédures d'audit prévues, les éléments probants qu'il recueille peuvent le conduire à modifier la nature, le calendrier ou l'étendue d'autres procédures prévues. Il peut prendre connaissance d'informations qui diffèrent sensiblement de celles sur lesquelles il s'est fondé pour son évaluation des risques. Par exemple :

- il peut arriver que l'étendue des anomalies détectées à l'occasion de la mise en œuvre de contrôles de substance amène l'auditeur à modifier son évaluation du risque et indique une déficience importante du contrôle interne ;
- l'auditeur peut découvrir des cas de non-concordance dans les documents comptables ou constater que certaines pièces justificatives sont manquantes ou contradictoires ;
- la mise en œuvre de procédures analytiques à l'étape de la revue d'ensemble de l'audit peut révéler l'existence d'un risque d'anomalies significatives passé jusque-là inaperçu.

En pareil cas, l'auditeur peut devoir réévaluer les procédures d'audit prévues, compte tenu de sa nouvelle évaluation des risques d'anomalies significatives et de l'incidence sur les relative à l'ensemble ou à une partie des flux d'opérations importants, des les soldes de comptes importants ou des les informations fournies à fournir importantes et des les assertions pertinentes les concernant sous-jacentes. La norme ISA 315 (révisée en 2019) donne de plus amples indications sur la révision de l'évaluation des risques par l'auditeur¹¹¹.

A61. L'auditeur ne peut présumer qu'un cas de fraude ou d'erreur est un fait isolé. C'est pourquoi, pour déterminer si son évaluation demeure valable ou non, il importe qu'il tienne compte des

¹¹¹ Norme ISA 315 (révisée en 2019), paragraphe 5334.

répercussions de la détection d'une anomalie sur son évaluation des risques d'anomalies significatives.

A62. Le jugement de l'auditeur quant au caractère suffisant et approprié des éléments probants est influencé notamment par les facteurs suivants :

- l'importance d'une anomalie potentielle dans une assertion et la probabilité que, seule ou cumulée avec d'autres, elle ait une incidence significative sur les états financiers ;
- l'efficacité des dispositions prises et des contrôles mis en œuvre par la direction pour répondre aux risques ;
- l'expérience acquise au cours des audits précédents concernant des anomalies potentielles similaires ;
- les résultats des procédures d'audit réalisées, selon notamment qu'elles ont permis de mettre en lumière ou non des cas précis de fraude ou d'erreur ;
- la source et la fiabilité des informations disponibles ;
- le caractère convaincant des éléments probants ;
- la connaissance de l'entité et de son environnement, ~~y compris de son~~ du référentiel comptable applicable et du système de contrôle interne de l'entité.

Documentation (Voir par. 28)

A63. La forme et l'étendue de la documentation de l'audit relèvent du jugement professionnel et varient selon la nature, la taille et la complexité de l'entité et de son système de contrôle interne, le degré de disponibilité des informations en provenance de l'entité ainsi que les méthodes et la technologie techniques d'audit employées au cours de l'audit.

Norme ISA 500, *Éléments probants*

Modalités d'application et autres commentaires explicatifs

Éléments probants suffisants et appropriés (Voir par. 6)

A1. Les éléments probants sont nécessaires pour étayer l'opinion et le rapport de l'auditeur. Les éléments probants sont cumulatifs par nature et sont principalement recueillis au moyen des procédures mises en œuvre au cours de l'audit. Cependant, ils peuvent également comprendre des informations obtenues d'autres sources telles que les audits antérieurs (sous réserve que l'auditeur ait ~~déterminé s'il est survenu depuis l'audit précédent des changements susceptibles d'affecter la pertinence de ces informations~~ évalué si, en tant qu'éléments probants pour l'audit en cours, ces informations demeurent pertinentes et fiables) ou les procédures de contrôle qualité appliquées par le cabinet pour l'acceptation ou le maintien d'une relation client. Les documents comptables de l'entité constituent une source importante d'éléments probants, parallèlement à d'autres sources internes ou externes à l'entité. Par ailleurs, certaines informations utilisables en tant qu'éléments probants peuvent avoir été produites à partir des travaux d'un expert choisi par la direction. Les éléments probants comprennent à la fois les informations qui étayent et corroborent les assertions de la direction et les informations qui les contredisent. De plus, dans certains cas, l'absence

d'information (par exemple, le refus de la direction de fournir une déclaration requise) est une information en elle-même pour l'auditeur, et constitue par conséquent un élément probant.

[...]

Procédures d'audit permettant l'obtention d'éléments probants

[...]

Observation physique

A17. L'observation physique consiste à examiner un processus ou une procédure en cours d'exécution par d'autres personnes. L'observation par l'auditeur de la prise d'inventaire effectuée par le personnel de l'entité ou l'observation de l'exécution des ~~mesures de contrôle~~ contrôles en sont des exemples. L'observation fournit des éléments probants en ce qui concerne l'exécution d'un processus ou d'une procédure, mais elle comporte des limites puisqu'elle ne vaut que pour le moment où l'observation a lieu et que le fait d'être observé peut affecter la manière dont le processus ou la procédure est exécuté. Pour des indications supplémentaires sur l'observation de la prise d'inventaire, voir la norme ISA 501.

Norme ISA 501, *Éléments probants — Considérations particulières concernant certains points*

Modalités d'application et autres commentaires explicatifs

Stocks

Présence à la prise d'inventaire physique (Voir par. 4 (a))

[...]

Évaluation des instructions et des procédures établies par la direction (Voir sous-paragraphe 4 (a)(i))

A4. Parmi les points à prendre en considération lors de l'évaluation des instructions et des procédures établies par la direction pour l'enregistrement et le contrôle de la prise d'inventaire physique de l'entité, il y a notamment le fait qu'elles prévoient ou non, par exemple :

- l'application de contrôles ~~à mise en œuvre d'mesures de contrôle~~ appropriées, en ce qui concerne entre autres la collecte des feuilles de comptage utilisées, le retour avec explications des feuilles de comptage inutilisées et les procédures de comptage et de recomptage ;

Norme ISA 530, *Sondages en audit*

Modalités d'application et autres commentaires explicatifs

[...]

Conception du sondage, taille de l'échantillon et sélection des éléments à tester

Conception du sondage (Voir par. 6)

[...]

- A7. Lors de la prise en considération des caractéristiques d'une population, dans le cas des tests de procédures, l'auditeur effectue une évaluation du taux d'écart attendu en se fondant sur sa connaissance des contrôles ~~pertinents~~ ou sur l'examen d'un petit nombre d'éléments de la population. Il s'appuie sur cette évaluation pour concevoir le sondage et décider de la taille de l'échantillon. [...]

Annexe 2
(Voir par. A11)

Exemples de facteurs influant sur la taille de l'échantillon dans le cas des tests de procédures

Pour déterminer la taille de l'échantillon dans le cas des tests de procédures, l'auditeur peut tenir compte des facteurs qui suivent. Ces facteurs doivent être considérés dans leur ensemble et, pour leur application, il est présumé que l'auditeur ne modifie pas la nature ni le calendrier des tests de procédures, ni la stratégie concernant les contrôles de substance qu'il a adoptés en réponse à son évaluation des risques.

Facteur 1 Augmentation de la mesure dans laquelle l'auditeur tient compte, pour son évaluation des risques, des tests d'efficacité du fonctionnement des contrôles qu'il prévoit de faire. ~~pertinents pour son évaluation des risques~~

Norme ISA 550, Parties liées

Modalités d'application et autres commentaires explicatifs

[...]

Procédures d'évaluation des risques et procédures liées

[...]

Connaissance des relations et opérations de l'entité avec des parties liées

Entretiens entre les membres de l'équipe affectés à la mission (Voir par. 12)

- A9. Les entretiens entre les membres de l'équipe affectés à la mission peuvent notamment porter sur les points suivants :

- [...]
- l'importance que la direction et les personnes constituant le gouvernement d'entreprise attachent à l'identification, au traitement comptable approprié et à la communication des relations et opérations avec les parties liées (lorsque le référentiel comptable applicable contient des diligences concernant les parties liées), et le risque connexe de contournement des contrôles ~~pertinents~~ par la direction.

[...]

L'identité des parties liées à l'entité (Voir par. 13 (a))

[...]

A12. En revanche, lorsque le référentiel ne contient pas d'diligences concernant les parties liées, il peut arriver que l'entité soit dépourvue de tels systèmes d'information. En pareille situation, la direction n'a pas nécessairement connaissance de l'existence de toutes les parties liées. Néanmoins, l'obligation de procéder aux demandes d'informations prescrites par le paragraphe 13 s'applique toujours parce qu'il se peut que la direction ait connaissance de l'existence de parties liées au sens de la présente norme ISA. En pareil cas, toutefois, il est probable que les demandes d'informations formulées par l'auditeur quant à l'identité des parties liées à l'entité feront partie des procédures d'évaluation des risques et des procédures liées qu'il met en œuvre conformément à la norme ISA 315 (révisée en 2019) afin d'obtenir des informations sur la structure organisationnelle de l'entité, son actionnariat, sa structure de gouvernance et son modèle économique.

- ~~le mode de propriété et la structure de gouvernance de l'entité ;~~
- ~~les types d'investissements réalisés et prévus par l'entité ;~~
- ~~l'organisation interne et les modes de financement de l'entité.~~

Dans le cas particulier des relations du fait d'un contrôle commun, comme la direction est d'autant plus susceptible d'avoir connaissance de telles relations qu'elles revêtent une importance économique pour l'entité, il est probable que les demandes d'informations de l'auditeur seront plus efficaces si elles sont axées sur la question de savoir si les parties avec lesquelles l'entité conclut des opérations importantes ou partage des ressources dans une mesure importante sont des parties liées.

[...]

Considérations propres aux petites entités

A20. Les contrôles ~~mesures de contrôle~~ des petites entités tendent à être moins formalisées et il peut arriver que celles-ci n'aient pas de processus documentés pour traiter les relations et opérations avec les parties liées. Un propriétaire exploitant peut atténuer certains des risques découlant des opérations avec les parties liées, ou au contraire potentiellement les accroître, de par sa participation active à l'ensemble des principaux aspects de ces opérations. Dans de telles entités, l'auditeur peut prendre connaissance des relations et opérations avec des parties liées ainsi que des contrôles qui peuvent exister à leur égard en combinant les demandes d'informations auprès de la direction avec d'autres procédures, comme l'observation des activités de surveillance et de revue menées par la direction et l'inspection de la documentation pertinente disponible.

[...]

Partage des informations sur les parties liées avec les autres membres de l'équipe affectés à la mission
(Voir par. 17)

A28. Constituent des exemples d'informations pertinentes sur les parties liées qui peuvent être partagées avec les autres membres de l'équipe affectés à la mission :

- l'identité des parties liées à l'entité ;
- la nature des relations et des opérations avec les parties liées ;
- les relations ou opérations importantes ou complexes avec les parties liées qui peuvent être identifiées comme des risques importants ~~exiger une attention spéciale lors de l'audit~~, notamment les opérations dans lesquelles la direction ou les personnes constituant le gouvernement d'entreprise sont impliqués financièrement.

[...]

Réponse à l'évaluation des risques d'anomalies significatives associés à des relations et opérations avec les parties liées (Voir par. 20)

[...]

A34. Selon les résultats de ses procédures d'évaluation des risques, l'auditeur peut considérer comme approprié de recueillir des éléments probants sans tester les contrôles de l'entité à l'égard des relations et opérations avec les parties liées. Dans certaines circonstances, toutefois, il se peut que les contrôles de substance ne permettent pas à eux seuls de recueillir des éléments probants suffisants et appropriés au sujet des risques d'anomalies significatives associés aux relations et opérations avec les parties liées. Par exemple, lorsque les opérations intragroupe entre l'entité et les autres composantes sont nombreuses et que des quantités importantes d'informations concernant ces opérations sont générées, enregistrées, traitées ou communiquées électroniquement dans un système intégré, il se peut que l'auditeur détermine qu'il n'est pas possible de concevoir des contrôles de substance qui, en eux-mêmes, réduiraient les risques d'anomalies significatives associés à ces opérations à un niveau suffisamment faible. En pareil cas, pour satisfaire à l'exigence de la norme ISA 330 qui lui impose de recueillir des éléments probants suffisants et appropriés sur l'efficacité du fonctionnement des contrôles pertinents¹¹², l'auditeur est tenu de tester les contrôles de l'entité visant à assurer l'exhaustivité et l'exactitude de l'enregistrement des relations et opérations avec les parties liées.

[...]

Norme ISA 540 (révisée), *Audit des estimations comptables et des informations y afférentes*

Introduction

Champ d'application de la présente norme ISA

1. La présente Norme internationale d'audit (ISA) traite des responsabilités de l'auditeur concernant les estimations comptables et les informations y afférentes dans le cadre d'un audit d'états financiers. Plus précisément, elle comporte des diligences et des indications sur l'application des normes

¹¹² Norme ISA 330, par. 8 (b).

ISA 315 (révisée en 2019)¹¹³, ISA 330¹¹⁴, ISA 450¹¹⁵ et ISA 500¹¹⁶, ainsi que d'autres normes ISA pertinentes, en ce qui a trait aux estimations comptables et aux informations y afférentes. Elle contient également des diligences et des indications relatives à l'évaluation des anomalies présentes dans les estimations comptables et les informations y afférentes, et à l'évaluation des indices d'un biais possible introduit par la direction.

Nature des estimations comptables

2. Les estimations comptables sont de nature très variable et doivent être établies par la direction pour les montants en numéraire qui ne sont pas directement observables. L'évaluation de ces montants comporte une incertitude d'estimation, qui reflète les limites inhérentes aux connaissances ou aux données – limites dont découlent nécessairement une part de subjectivité et une variabilité des résultats de l'évaluation. Le processus d'établissement d'estimations comptables consiste à choisir et à appliquer une méthode en fonction d'hypothèses et de données, ce qui nécessite de la direction qu'elle exerce son jugement et peut rendre l'évaluation complexe. Les incidences de la complexité, de la subjectivité et des autres facteurs de risque inhérent sur l'évaluation de ces montants en numéraire influent sur leur vulnérabilité aux anomalies. (Voir par. A1–A6 et Annexe 1)
3. La présente norme ISA s'applique à toutes les estimations comptables. Cela dit, le degré d'incertitude d'estimation que celles-ci comporteront sera très variable. La nature, le calendrier et l'étendue des procédures d'évaluation des risques et des procédures d'audit complémentaires exigées par la présente norme ISA dépendront de l'incertitude d'estimation et de l'évaluation des risques d'anomalies significatives s'y rattachant. Il arrive que des estimations comptables comportent par nature une incertitude d'estimation très faible, et que le degré de complexité et de subjectivité de leur établissement soit aussi très faible. Pour ces estimations comptables, les procédures d'évaluation des risques et les procédures d'audit complémentaires exigées par la présente norme ISA ne devraient pas être très poussées. Si, au contraire, le degré d'incertitude d'estimation, de complexité ou de subjectivité est très élevé, on peut s'attendre à ce que les procédures soient beaucoup plus poussées. La présente norme ISA donne des indications sur la façon d'en adapter les diligences. (Voir par. A7)

Concepts fondamentaux de la présente norme ISA

4. La ~~présente~~ norme ISA 315 (révisée en 2019) requiert que le risque inhérent soit évalué séparément en ce qui concerne les ~~lors de l'évaluation des risques~~ d'anomalies significatives identifiés au niveau des assertions¹¹⁷ ~~liés aux estimations comptables~~. Dans le contexte de la norme ISA 540 (révisée), et s selon la nature de l'estimation comptable, il se peut que l'incertitude d'estimation, la complexité, la subjectivité ou d'autres facteurs de risque inhérent, ainsi que leurs interrelations, aient une incidence sur la possibilité qu'une assertion comporte une anomalie qui pourrait être significative. Comme il est expliqué dans la norme ISA 200¹¹⁸, le risque inhérent est plus élevé pour certaines

¹¹³ Norme ISA 315 (révisée en 2019), *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives*.

¹¹⁴ Norme ISA 330, *Réponses de l'auditeur à l'évaluation des risques*.

¹¹⁵ Norme ISA 450, *Évaluation des anomalies détectées au cours de l'audit*.

¹¹⁶ Norme ISA 500, *Éléments probants*.

¹¹⁷ Norme ISA 315 (révisée en 2019), *paragraphe 31*.

¹¹⁸ Norme ISA 200, *Objectifs généraux de l'auditeur indépendant et réalisation d'un audit conforme aux Normes internationales d'audit*, paragraphe A40.

assertions et pour les flux d'opérations, soldes de comptes ou informations à fournir ~~qui s'y rapportent concernés~~ que pour d'autres. L'évaluation du risque inhérent dépend donc de la mesure dans laquelle les facteurs de risque inhérent influent sur la probabilité ou l'ampleur d'une anomalie, et s'inscrit sur une échelle appelée « échelle de risque inhérent » ~~dans la présente norme ISA~~. (Voir par. A8–A9, A65–A66, et Annexe 1)

5. La présente norme ISA renvoie aux diligences pertinentes des normes ISA 315 (révisée en 2019) et ISA 330, et fournit des indications connexes, pour souligner l'importance des décisions que prend l'auditeur quant aux contrôles liés aux estimations comptables, notamment lorsqu'il :
 - détermine s'il existe des contrôles ~~pertinents pour l'audit~~ qui doivent être identifiés selon la norme ISA 315 (révisée en 2019), l'auditeur étant tenu d'évaluer la conception de ces contrôles et de déterminer s'ils ont été mis en œuvre ;
 - décide de tester ou non l'efficacité du fonctionnement des contrôles ~~pertinents~~.
6. La ~~présente~~ norme ISA 315 (révisée en 2019) requiert aussi que le risque lié au contrôle interne soit évalué séparément lors de l'évaluation des risques d'anomalies significatives au niveau des assertions ~~liés aux estimations comptables~~. Lorsqu'il évalue le risque lié au contrôle interne, l'auditeur se demande si les procédures d'audit complémentaires qu'il prévoit de mettre en œuvre impliquent qu'il s'appuie sur l'efficacité du fonctionnement des contrôles. S'il ne prévoit pas de tester l'efficacité du fonctionnement ~~l'auditeur ne met pas en œuvre de tests des contrôles, ou qu'il ne compte pas s'appuyer sur l'efficacité du fonctionnement des contrôles, il ne saurait s'appuyer sur l'efficacité du fonctionnement des contrôles pour réviser à la baisse son~~ l'évaluation du risque lié au contrôle interne doit faire en sorte que l'évaluation du risque d'anomalies significatives corresponde à l'évaluation du risque inhérent au niveau des assertions en ce qui concerne une assertion particulière⁴⁴⁹. (Voir par. A10)
7. La présente norme ISA souligne que les procédures d'audit complémentaires mises en œuvre par l'auditeur (notamment, s'il y a lieu, les tests de procédures) doivent être adaptées aux raisons qui sous-tendent l'évaluation des risques d'anomalies significatives au niveau des assertions, et prendre en compte l'effet d'un ou de plusieurs facteurs de risque inhérent et l'évaluation par l'auditeur du risque lié au contrôle interne.
8. L'exercice de l'esprit critique à l'égard des estimations comptables est influencé par la prise en compte, par l'auditeur, des facteurs de risque inhérent, et son importance s'accroît lorsque les estimations comptables comportent un degré élevé d'incertitude d'estimation, ou sont fortement touchées par la complexité, la subjectivité ou d'autres facteurs de risque inhérent. De même, l'exercice de l'esprit critique est important dans les cas où la vulnérabilité aux anomalies résultant de partis pris de la direction ou d'autres facteurs de risque de fraudes, ~~dans la mesure où ils influent sur le risque inhérent~~, est particulièrement grande. (Voir par. A11)

[...]

Objectif

[...]

⁴⁴⁹ Norme ISA 530, *Sondages en audit*, Annexe 3.

Définitions

[...]

Diligences

Procédures d'évaluation des risques et procédures liées

13. Lorsqu'il acquiert une connaissance de l'entité et de son environnement, du référentiel comptable applicable et y compris du système de contrôle interne de l'entité, comme le requiert la norme ISA 315 (révisée en 2019)¹²⁰, l'auditeur doit prendre connaissance des points indiqués ci-après en ce qui a trait aux estimations comptables de l'entité. Les procédures qu'il met en œuvre afin d'acquérir cette connaissance doivent être suffisantes pour lui permettre de recueillir des éléments probants qui fourniront une base appropriée aux fins de l'identification et de l'évaluation des risques d'anomalies significatives aux niveaux des états financiers et au niveau des assertions. (Voir par. A19–A22)

Prise de connaissance de l'entité et de son environnement et du référentiel comptable applicable

- (a) Les opérations de l'entité et les autres événements ~~et ou~~ situations pouvant nécessiter la comptabilisation d'estimations comptables ou la fourniture d'informations y afférentes dans les états financiers, ou entraîner des changements dans ces estimations. (Voir par. A23)
- (b) Les diligences du référentiel comptable applicable relatives aux estimations comptables (notamment les critères de comptabilisation et les bases d'évaluation à utiliser, ainsi que les diligences connexes en matière de présentation et d'informations à fournir) et leur application au regard de la nature et des circonstances de l'entité et de son environnement, y compris l'incidence des facteurs de risque inhérent sur ~~les opérations et les autres événements et situations~~ la possibilité que les assertions comportent des anomalies. (Voir par. A24–A25)
- (c) Les facteurs réglementaires pertinents en ce qui a trait aux estimations comptables de l'entité, y compris, s'il y a lieu, les cadres réglementaires relatifs au contrôle prudentiel. (Voir par. A26)
- (d) La nature des estimations comptables et des informations y afférentes que l'auditeur s'attend à trouver dans les états financiers de l'entité, selon sa connaissance des points mentionnés aux paragraphes (a)–(c) ci-dessus. (Voir par. A27)

Prise de connaissance du système de ~~Le~~ contrôle interne de l'entité

- (e) La nature et l'étendue de la surveillance et de la gouvernance que l'entité exerce sur le processus d'information financière de la direction en ce qui a trait aux estimations comptables. (Voir par. A28–A30)
- (f) La manière dont la direction détermine et applique les compétences ou les connaissances spécialisées que nécessitent les estimations comptables, et identifie le besoin de recourir à un expert de son choix. (Voir par. A31)
- (g) La manière dont le processus d'évaluation des risques par l'entité permet d'identifier les risques liés aux estimations comptables et d'y répondre. (Voir par. A32–A33)

¹²⁰ Norme ISA 315 (révisée en 2019), paragraphes 3, 5, 6, 9, 11, 12, 15 à 17, 20 et 24 à 27.

- (h) Le système d'information de l'entité en ce qui a trait aux estimations comptables, notamment :
- (i) ~~le flux, dans le système d'information de l'entité, des informations relatives aux estimations comptables et des informations y afférentes pour les flux d'opérations importants, les soldes de comptes importants et les informations à fournir importantes les flux d'opérations, les événements et les situations qui sont importants par rapport aux états financiers et qui nécessitent la comptabilisation d'estimations comptables ou la fourniture d'informations y afférentes, ou entraînent des changements dans ces estimations ou informations;~~ (Voir par. A34–A35)
 - (ii) pour ces estimations comptables et les informations y afférentes, la manière dont la direction :
 - a. identifie les méthodes, les hypothèses et les sources de données pertinentes qui sont appropriées au regard du référentiel comptable applicable, et détermine la nécessité de les modifier, ce qui comprend la façon dont elle : (Voir par. A36– A37)
 - i. choisit ou conçoit, et applique les méthodes, y compris en ce qui concerne l'utilisation de modèles, (Voir par. A38–A39)
 - ii. choisit les hypothèses à utiliser, en tenant compte des autres hypothèses possibles, et identifie celles qui sont importantes, (Voir par. A40–A43)
 - iii. choisit les données à utiliser, (Voir par. A44)
 - b. acquiert une connaissance du degré d'incertitude d'estimation, notamment par la prise en compte de la fourchette des résultats possibles de l'évaluation, (Voir par. A45)
 - c. répond à l'incertitude d'estimation, notamment la manière dont elle choisit l'estimation ponctuelle et les informations y afférentes à inclure dans les états financiers. (Voir par. A46–A49)
- (i) Les contrôles identifiés de la composante « mesures de contrôle »¹²¹ ~~pertinentes pour l'audit~~ qui concernent le processus d'établissement des estimations comptables par la direction dont il est question au sous-paragraphe 13 (h)(ii). (Voir par. A50–A54)
- (j) La manière dont la direction examine le dénouement des estimations comptables antérieures et donne suite aux résultats de cet examen.
14. L'auditeur doit examiner le dénouement des estimations comptables antérieures ou, s'il y a lieu, leur révision subséquente, afin qu'il lui soit plus facile d'identifier et d'évaluer les risques d'anomalies significatives pour la période en cours. Lorsqu'il détermine la nature et l'étendue de cet examen, l'auditeur doit tenir compte des caractéristiques des estimations comptables. Cet examen n'a pas pour objet de remettre en cause les jugements portés quant aux estimations comptables des périodes précédentes qui étaient appropriés compte tenu des informations disponibles au moment où ils ont été portés. (Voir par. A55–A60)

¹²¹ Norme ISA 315 (révisée en 2019), sous-par. s 26 (a)(i)–(iv).

[...]

Identification et évaluation des risques d'anomalies significatives

16. Lorsqu'il identifie et évalue les risques d'anomalies significatives au niveau des assertions liés à une estimation comptable et aux informations y afférentes et, ce faisant, évalue séparément le risque inhérent et le risque lié au contrôle interne, comme l'exige la norme ISA 315 (révisée en 2019)¹²², l'auditeur doit ~~procéder à une évaluation séparée du risque inhérent et du risque lié au contrôle~~. L'auditeur doit tenir compte de ce qui suit pour l'identification des risques d'anomalies significatives et pour l'évaluation du risque inhérent : (Voir par. A64–A71)
- (a) le degré d'incertitude d'estimation que comportent les estimations comptables ; (Voir par. A72– A75)
 - (b) la mesure dans laquelle la complexité, la subjectivité ou d'autres facteurs de risque inhérent ont une incidence sur : (Voir par. A76–A79)
 - (i) le choix et l'application de la méthode, des hypothèses et des données pour l'établissement des estimations comptables,
 - (ii) le choix de l'estimation ponctuelle de la direction et des informations y afférentes à inclure dans les états financiers.
17. L'auditeur doit déterminer si, selon son jugement, il y a des risques importants parmi les risques d'anomalies significatives identifiés et évalués conformément au paragraphe 16¹²³. Si l'auditeur a déterminé qu'il existe un risque important, il doit identifier les contrôles qui répondent ~~prendre connaissance des contrôles de l'entité, y compris des mesures de contrôle, pertinents par rapport à~~ ce risque¹²⁴, puis évaluer si leur conception est efficace et déterminer s'ils ont été mis en œuvre¹²⁵. (Voir par. A80)

[...]

19. Comme le requiert la norme ISA 330¹²⁶, l'auditeur doit concevoir et mettre en œuvre des tests à l'égard des contrôles ~~pertinents~~ de manière à recueillir des éléments probants suffisants et appropriés sur l'efficacité de leur fonctionnement dans l'un ou l'autre des cas suivants :
- (a) son évaluation des risques d'anomalies significatives au niveau des assertions repose sur l'attente d'un fonctionnement efficace des contrôles ;
 - (b) les contrôles de substance ne peuvent fournir à eux seuls des éléments probants suffisants et appropriés au niveau des assertions.

En ce qui concerne les estimations comptables, les tests mis en œuvre par l'auditeur à l'égard de ces contrôles doivent être adaptés aux raisons qui sous-tendent l'évaluation des risques d'anomalies significatives. Lors de la conception et de la mise en œuvre des tests de procédures, l'auditeur doit

¹²² Norme ISA 315 (révisée en 2019), paragraphes ~~25 et 26~~ 31 et 34.

¹²³ Norme ISA 315 (révisée en 2019), paragraphe 3227.

¹²⁴ Norme ISA 315 (révisée en 2019), sous-par. 26 (a)(i) ~~paragraphe 29~~.

¹²⁵ Norme ISA 315 (révisée en 2019), par. 26 (a).

¹²⁶ Norme ISA 330, paragraphe 8.

recueillir des éléments probants d'autant plus convaincants qu'il s'appuie sur l'efficacité des contrôles¹²⁷. (Voir par. A85–A89)

[...]

Autres considérations liées aux éléments probants

30. Pour recueillir des éléments probants sur les risques d'anomalies significatives liés aux estimations comptables, quelles que soient les sources des informations devant servir d'éléments probants, l'auditeur doit se conformer aux diligences pertinentes de la norme ISA 500.

Lorsque l'auditeur utilise les travaux d'un expert choisi par la direction, les diligences des paragraphes 21–29 de la présente norme ISA peuvent l'aider à évaluer le caractère approprié des travaux de l'expert devant servir d'éléments probants pour l'assertion concernée, conformément au paragraphe 8 (c) de la norme ISA 500. Dans le cadre de l'évaluation des travaux de l'expert choisi par la direction, la nature, le calendrier et l'étendue des procédures d'audit complémentaires sont influencés par l'évaluation, par l'auditeur, de la compétence, des capacités et de l'objectivité de l'expert, par sa connaissance de la nature des travaux effectués par l'expert, et par le niveau de ses connaissances dans le domaine d'expertise de l'expert. (Voir par. A126–A132)

[...]

Documentation

39. L'auditeur doit inclure dans la documentation de l'audit¹²⁸ : (Voir par. A149–A152)
- (a) les éléments clés de sa connaissance de l'entité et de son environnement, y compris son contrôle interne par rapport aux estimations comptables ;
 - (b) le lien entre les procédures d'audit complémentaires mises en œuvre et son évaluation des risques d'anomalies significatives au niveau des assertions¹²⁹, compte tenu des raisons (qu'elles aient trait au risque inhérent ou au risque lié au contrôle interne) qui sous-tendent cette évaluation ;
 - (c) la ou les mesures qu'il a appliquées dans les cas où la direction n'a pas pris des moyens appropriés pour comprendre l'incertitude d'estimation ou y répondre ;
 - (d) les indices d'un biais possible introduit par la direction relativement aux estimations comptables, le cas échéant, et son évaluation des incidences sur l'audit conformément au paragraphe 32 ;
 - (e) les jugements importants à partir desquels il a déterminé si les estimations comptables et les informations y afférentes étaient raisonnables au regard du référentiel comptable applicable, ou si elles comportaient des anomalies.

Modalités d'application et autres commentaires explicatifs

¹²⁷ Norme ISA 330, paragraphe 9.

¹²⁸ Norme ISA 230, *Documentation de l'audit*, paragraphes 8–11, A6, A7 et A10.

¹²⁹ Norme ISA 330, par. 28 (b).

Nature des estimations comptables (Voir par. 2)

Exemples d'estimations comptables

[...]

Méthodes

A2. Une méthode est une technique d'évaluation que la direction utilise pour établir une estimation comptable selon la base d'évaluation exigée. Par exemple, l'une des méthodes reconnues aux fins de l'établissement d'estimations comptables liées à des opérations dont le paiement est fondé sur des actions consiste à déterminer le prix théorique d'une option d'achat au moyen de la formule d'évaluation des options de Black-Scholes. Une méthode se met en œuvre au moyen d'un outil ou d'un procédé de calcul – qu'on appelle parfois un modèle –, et implique l'utilisation d'hypothèses et de données ainsi que la prise en compte d'un ensemble de liens entre elles.

Hypothèses et données

A3. Les hypothèses impliquent de porter des jugements, à partir des informations disponibles, sur des éléments comme le choix d'un taux d'intérêt ou d'un taux d'actualisation, ou sur des situations ou événements futurs. La direction peut choisir une hypothèse parmi un éventail de possibilités appropriées. Les hypothèses élaborées ou retenues par un expert choisi par la direction deviennent celles de la direction lorsque celle-ci les utilise pour établir une estimation comptable.

A4. Dans la présente norme ISA, le terme « données » s'entend d'informations qui peuvent être obtenues au moyen d'une observation directe ou auprès d'une partie extérieure à l'entité. Les informations obtenues par l'application, à des données, de techniques analytiques ou de techniques d'interprétation sont appelées « données dérivées » lorsque les techniques en question ont un fondement théorique solide et que, par conséquent, elles font appel dans une moindre mesure au jugement de la direction. Autrement, ces informations constituent des hypothèses.

A5. Voici quelques exemples de données :

- les prix convenus lors d'opérations sur le marché ;
- la durée de fonctionnement d'une machine ou le nombre d'unités produites par celle-ci ;
- les prix historiques ou d'autres modalités contractuelles, par exemple, le taux d'intérêt, le calendrier de paiement ou l'échéance stipulés dans un contrat de prêt ;
- les informations prospectives, par exemple les prévisions de conjoncture économique ou de résultats obtenues auprès d'une source d'informations externe ;
- un taux d'intérêt futur déterminé au moyen de techniques d'interpolation à partir des taux d'intérêt à terme (données dérivées).

A6. Les données peuvent provenir d'une grande variété de sources. Par exemple, elles peuvent être :

- générées en interne ou en externe ;
- produites par un système qui fait partie ou non du grand livre et des journaux auxiliaires ;
- observables dans des contrats ;

- observables dans des prises de position législatives ou réglementaires.

Application proportionnée (Voir par. 3)

A7. Les paragraphes A20–A22, A63, A67 et A84, notamment, donnent des indications sur la façon d'adapter les diligences de la présente norme ISA.

Concepts fondamentaux de la présente norme ISA

Facteurs de risque inhérent (Voir par. 4)

A8. Les facteurs de risque inhérent sont ~~des~~ caractéristiques, ~~de situations ou d'~~des événements ou situations ayant qui peuvent avoir une incidence sur la possibilité qu'une assertion portant sur un flux 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 prise en considération des contrôles¹³⁰. L'Annexe 1 explique de façon plus détaillée la nature de ces facteurs de risque inhérent, ainsi que leurs interrelations, au regard de l'établissement d'estimations comptables et de leur présentation dans les états financiers.

A9. ~~Outre l'incertitude d'estimation, la complexité et la subjectivité~~ Lorsqu'il évalue les risques d'anomalies significatives au niveau des assertions¹³¹, l'auditeur ~~peut tenir~~ tient aussi compte de la mesure dans laquelle ~~d'les autres~~ facteurs de risque inhérent (outre l'incertitude d'estimation, la complexité et la subjectivité) mentionnés dans la norme ISA 315 (révisée en 2019) ~~lors de l'identification et de l'évaluation des risques d'influent sur la possibilité que les assertions portant sur des estimations comptables comportent des anomalies~~. Voici des exemples de tels facteurs de risque inhérent significatives, notamment la mesure dans laquelle les estimations comptables sont touchées par :

- des changements de nature ou de circonstances qui concernent des éléments pertinents des états financiers ou des diligences du référentiel comptable applicable et qui sont susceptibles de nécessiter une modification de la méthode, des hypothèses ou des données utilisées aux fins de l'établissement des estimations comptables ;
- la possibilité d'anomalies résultant de biais introduits par la direction ou d'autres facteurs de risque de fraude, dans la mesure où ils influent sur le risque inhérent, lors de l'établissement des estimations comptables ;
- l'incertitude, autre que l'incertitude d'estimation.

Risque lié au contrôle interne (Voir par. 6)

A10. Lors de l'évaluation du risque lié au contrôle interne au niveau des assertions selon la norme ISA 315 (révisée en 2019), il est important que l'auditeur tienne compte ~~de du~~ fait qu'il prévoit ou non de tester l'efficacité de la conception du fonctionnement des contrôles ~~sur lesquels il a l'intention de s'appuyer et de la mesure dans laquelle les contrôles répondent à l'évaluation des risques inhérents~~

¹³⁰ Norme ISA 315 (révisée en 2019), par. 12 (f)

¹³¹ Norme ISA 315 (révisée en 2019), paragraphe 31.

~~au niveau des assertions. Lorsque l'auditeur se demande s'il doit tester l'efficacité du fonctionnement des contrôles, L'son évaluation de l'efficacité de la conception et la vérification de la mise en œuvre des contrôles lui permettent à l'auditeur de fonder son attente quant à l'efficacité du fonctionnement de ces contrôles – attente qui lui servira à déterminer s'il y a lieu de tester les~~ planifier ses tests de procédures.

Esprit critique (Voir par. 8)

[...]

Notion de « caractère raisonnable » (Voir par. 9 et 35)

[...]

Procédures d'évaluation des risques et procédures liées

Prise de connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité (Voir par. 13)

A19. Selon les paragraphes ~~19–2744–24~~ de la norme ISA 315 (révisée en 2019), l'auditeur doit prendre connaissance de certains points concernant l'entité et son environnement, le référentiel comptable applicable et le système de y compris son contrôle interne de l'entité. Les diligences du paragraphe 13 de la présente norme ISA visent plus précisément les estimations comptables et s'ajoutent aux diligences générales de la norme ISA 315 (révisée en 2019).

Application proportionnée

A20. La nature, le calendrier et l'étendue des procédures que l'auditeur met en œuvre pour prendre connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système y compris de son contrôle interne de l'entité, par rapport aux estimations comptables, peuvent dépendre à des degrés divers de la mesure dans laquelle chacun des points s'applique dans les circonstances. Par exemple, il peut y avoir, pour une entité donnée, peu d'opérations ou d'autres événements ou situations rendant nécessaire l'établissement d'estimations comptables, et il se peut que les obligations d'information financière applicables soient simples à remplir et qu'il n'existe pas de facteurs réglementaires pertinents. En outre, il se peut que l'établissement des estimations comptables ne nécessite pas de porter des jugements importants et que ce processus soit simple. Dans ces circonstances, il est possible que les estimations comptables ne soient touchées que dans une moindre mesure par l'incertitude d'estimation, la complexité, la subjectivité ou d'autres facteurs de risque inhérent, et que les contrôles identifiés de la composante « mesures de contrôle » pertinents pour l'audit soient peu nombreux. Le cas échéant, les procédures d'identification et d'évaluation des risques mises en œuvre par l'auditeur seront probablement moins poussées et pourront consister principalement en des demandes d'informations à des membres de la direction qui sont investis de responsabilités appropriées à l'égard des états financiers ~~et en~~ ; il pourrait s'agir par exemple des tests de cheminement du processus qu'a suivi la direction pour établir les estimations comptables (notamment lorsque l'auditeur évalue l'efficacité de la conception des contrôles identifiés pour ce processus et qu'il détermine si ces contrôles ont été mis en œuvre).

- A21. À l'inverse, il se peut que l'établissement des estimations comptables nécessite que la direction porte des jugements importants, et que ce processus ne soit pas simple et implique l'utilisation de modèles complexes. De plus, l'entité peut avoir mis en œuvre un système d'information sophistiqué et des contrôles poussés à l'égard des estimations comptables. Dans ces circonstances, il est possible que les estimations comptables soient touchées dans une plus large mesure par l'incertitude d'estimation, la subjectivité, la complexité ou d'autres facteurs de risque inhérent. Le cas échéant, la nature ou le calendrier des procédures d'évaluation des risques mises en œuvre par l'auditeur ne seront probablement pas les mêmes, et ces procédures seront probablement plus poussées, que dans les circonstances mentionnées au paragraphe A20.
- A22. Les considérations suivantes peuvent être pertinentes pour les entités qui ne mènent que des activités simples, ce qui est le cas de beaucoup de petites entités :
- Il se peut que les processus pertinents en ce qui a trait aux estimations comptables ne soient pas compliqués parce que les activités de l'entité sont simples ou que les estimations nécessaires comportent un faible degré d'incertitude d'estimation.
 - Il est possible que les estimations comptables soient générées hors du grand livre et des journaux auxiliaires, que leur établissement fasse l'objet de contrôles restreints et qu'il soit influencé de façon notable par le propriétaire-dirigeant. L'auditeur pourrait devoir tenir compte du rôle du propriétaire-dirigeant dans l'établissement des estimations comptables lors de l'identification des risques d'anomalies significatives et de la prise en considération du risque de biais introduit par la direction.

L'entité et son environnement

Les opérations de l'entité et les autres événements ~~et~~ou situations (Voir par. 13 (a))

- A23. Voici des exemples de changements de circonstances susceptibles de nécessiter l'établissement ou la révision d'estimations comptables :
- l'entité s'est engagée dans de nouveaux types d'opérations ;
 - les modalités des opérations ont changé ;
 - de nouveaux événements ou de nouvelles situations se sont produits.

Les diligences du référentiel comptable applicable (Voir par. 13 (b))

- A24. La connaissance des diligences du référentiel comptable applicable fournit à l'auditeur une base sur laquelle s'appuyer pour s'entretenir avec la direction et, s'il y a lieu, les personnes constituant le gouvernement d'entreprise, de la manière dont la direction a appliqué les diligences du référentiel comptable applicable relatives aux estimations comptables et de la question de savoir s'il considère que ces diligences ont été appliquées adéquatement. Cette connaissance peut également aider l'auditeur à communiquer avec les personnes constituant le gouvernement d'entreprise lorsqu'il juge qu'une pratique comptable importante, qui est par ailleurs acceptable selon le référentiel comptable applicable, n'est pas la plus appropriée aux circonstances de l'entité¹³².

¹³² Norme ISA 260 (révisée), par. 16 (a).

A25. Pour acquérir cette connaissance, l'auditeur peut chercher à comprendre si :

- le référentiel comptable applicable :
 - prescrit des critères de comptabilisation ou des méthodes d'évaluation pour les estimations comptables,
 - précise les critères selon lesquels l'évaluation à la juste valeur est permise ou exigée, par exemple en fonction des intentions de la direction de mener à bien certaines actions envisagées par rapport à un actif ou à un passif,
 - précise les informations qu'il est obligatoire ou suggéré de fournir, notamment en ce qui concerne les jugements, les hypothèses ou d'autres sources d'incertitude d'estimation liée aux estimations comptables ;
- des changements dans le référentiel comptable applicable exigent la modification des méthodes comptables de l'entité qui concernent les estimations comptables.

Les facteurs réglementaires (Voir par. 13 (c))

[...]

La nature des estimations comptables et des informations y afférentes que l'auditeur s'attend à trouver dans les états financiers (Voir par. 13 (d))

[...]

~~Les aspects du système de contrôle interne de l'entité pertinents pour l'audit~~

La nature et l'étendue de la surveillance et de la gouvernance (Voir par. 13 (e))

A28. La connaissance qu'acquiert l'auditeur de la nature et de l'étendue de la surveillance et de la gouvernance mises en œuvre par l'entité à l'égard du processus d'information financière de la direction en ce qui a trait aux estimations comptables peut s'avérer importante aux fins de l'application de la norme ISA 315 (révisée en 2019)¹³³, qui requiert de l'auditeur qu'il évalue :

- si la direction, sous la surveillance des personnes constituant le gouvernement d'entreprise, a développé et entretient une culture d'honnêteté et de comportement éthique ;
- ~~si les points forts des éléments de l'environnement de contrôle constituent collectivement~~ fournit une base appropriée, compte tenu de la nature et de la taille de l'entité, sur laquelle peuvent s'appuyer les autres composantes du système de contrôle interne ;
- ~~et si l'efficacité de ces autres composantes est réduite par des~~ les déficiences de contrôle relevées dans l'environnement de contrôle nuisent aux autres composantes du système de contrôle interne.

[...]

¹³³ Norme ISA 315 (révisée en 2019), paragraphe 14 par. 21 (a)

A30. La connaissance de la surveillance exercée par les personnes constituant le gouvernement d'entreprise peut être importante en présence d'estimations comptables :

- qui font largement appel au jugement de la direction en raison de leur subjectivité ;
- qui comportent un degré élevé d'incertitude d'estimation ;
- dont l'établissement est complexe, par exemple parce qu'il repose largement sur le recours à l'informatique, qu'il nécessite un volume important de données, ou qu'il implique l'utilisation de plusieurs sources de données ou de plusieurs hypothèses ayant des interrelations complexes ;
- qui sont fondées sur une méthode, des hypothèses ou des données qui ont changé ou auraient dû changer par rapport aux périodes précédentes ;
- qui impliquent des hypothèses importantes.

L'application de compétences ou de connaissances spécialisées par la direction, y compris le recours aux services d'un expert de son choix (Voir par. 13 (f))

[...]

Le processus d'évaluation des risques par l'entité (Voir par. 13(g))

A32. La connaissance de la manière dont le processus d'évaluation des risques par l'entité permet d'identifier les risques liés aux estimations comptables et d'y répondre peut aider l'auditeur à prendre en considération les changements liés :

- aux diligences du référentiel comptable applicable qui concernent les estimations comptables ;
- à la disponibilité ou à la nature des sources de données qui sont pertinentes aux fins de l'établissement des estimations comptables ou qui peuvent influencer sur la fiabilité des données utilisées ;
- aux systèmes d'information ou à l'environnement informatique de l'entité ;
- au personnel clé.

A33. Pour prendre connaissance de la manière dont la direction a identifié et répond à la vulnérabilité aux anomalies résultant de ses propres partis pris ou de fraudes dans le cadre de l'établissement des estimations comptables, l'auditeur peut, par exemple, se demander si et, le cas échéant, comment la direction :

- accorde une attention particulière au choix et à l'application des méthodes, des hypothèses et des données qu'elle utilise pour établir les estimations comptables ;
- fait un suivi des indicateurs clés de performance qui peuvent indiquer une performance inattendue ou incohérente par rapport à la performance historique ou prévue ou à d'autres facteurs connus ;
- identifie les motifs financiers ou autres qui pourraient entraîner des partis pris ;
- fait un suivi pour déterminer s'il est nécessaire d'apporter des changements aux méthodes, aux hypothèses importantes ou aux données utilisées aux fins de l'établissement des estimations comptables ;

- met en œuvre des processus appropriés de surveillance et d'examen des modèles utilisés aux fins de l'établissement des estimations comptables ;
- requiert que soit consigné le raisonnement qui sous-tend les jugements importants portés aux fins de l'établissement des estimations comptables, ou que ces jugements fassent l'objet d'un examen indépendant.

Système d'information de l'entité en ce qui a trait aux estimations comptables (Voir par. 13 (h)(i))

A34. Les flux d'opérations importants, les événements importants et les situations importantes auxquels s'applique le paragraphe 13 (h) sont les mêmes que ceux, liés aux estimations comptables et aux informations y afférentes, qui sont visés par ~~les le~~ paragraphes 1825 (a) et d) de la norme ISA 315 (révisée en 2019). Pour prendre connaissance du système d'information de l'entité en ce qui a trait aux estimations comptables, l'auditeur peut prendre en considération :

- le fait que les estimations comptables découlent de l'enregistrement d'opérations courantes et récurrentes ou, au contraire, d'opérations non récurrentes ou inhabituelles ;
- la manière dont le système d'information permet d'assurer l'exhaustivité des estimations comptables et des informations y afférentes, en particulier dans le cas des estimations comptables liées aux passifs.

A35. Au cours de l'audit, il peut arriver que l'auditeur découvre des flux d'opérations, des événements ou des situations qui nécessitent des estimations comptables et la fourniture d'informations y afférentes, mais qui n'ont pas été identifiés par la direction. La norme ISA 315 (révisée en 2019) traite des circonstances où l'auditeur identifie des risques d'anomalies significatives que la direction n'a pas identifiés, et notamment de la ~~détermination de l'existence ou non d'une déficience importante du contrôle interne en ce qui concerne le~~ prise en compte des conséquences sur son appréciation du processus d'évaluation des risques par l'entité¹³⁴.

Identification par la direction des méthodes, des hypothèses et des sources de données pertinentes (Voir par. 13 (h)(ii)a.)

[...]

Méthodes (Voir par. 13 (h)(ii)a.i.)

[...]

Modèles

A39. La direction peut concevoir et mettre en œuvre des contrôles portant précisément sur les modèles utilisés aux fins de l'établissement d'estimations comptables, qu'il s'agisse de modèles élaborés par la direction ou de modèles externes. Lorsque le modèle lui-même comporte un degré élevé de complexité ou de subjectivité, comme ce peut être le cas par exemple d'un modèle d'évaluation des pertes de crédit attendues ou d'un modèle servant à déterminer la juste valeur à partir de données d'entrée de niveau 3, il se peut que les contrôles qui répondent à cette complexité ou subjectivité soient. De même, la complexité du modèle fait augmenter la probabilité que les contrôles visant à

¹³⁴ Norme ISA 315 (révisée en 2019), ~~paragraphe par.~~ 4322 (b)

assurer l'intégrité des données soient des contrôles identifiés en application de la norme ISA 315 (révisée en 2019) pertinents pour l'audit. Des facteurs appropriés que l'auditeur peut considérer lors de la prise de connaissance du modèle et des contrôles ~~mesures de contrôle~~ identifiés s'y rapportant pertinents pour l'audit, incluent, par exemple :

- comment la direction détermine la pertinence et l'exactitude du modèle ;
- si le modèle fait l'objet d'une validation, ou d'un contrôle a posteriori, et s'il est validé avant utilisation puis à intervalles réguliers pour qu'on puisse déterminer s'il est toujours adapté à son objectif. Le processus de validation de l'entité peut notamment comprendre une évaluation :
 - de la robustesse théorique du modèle,
 - de la rigueur mathématique du modèle,
 - de l'exactitude et de l'exhaustivité des données, ainsi que du caractère approprié des données et des hypothèses utilisées dans le modèle ;
- comment les modifications ou les ajustements appropriés sont apportés au modèle en temps opportun pour refléter l'évolution des conditions de marché ou d'autres facteurs, et s'il existe des politiques appropriées pour le contrôle des modifications apportées au modèle ;
- si des ajustements (par exemple, ceux qui découlent de l'application, dans certains secteurs d'activité, de l'approche par superposition) sont apportés aux données de sortie du modèle, et si ces ajustements sont appropriés dans les circonstances et respectent les diligences du référentiel comptable applicable. Lorsque les ajustements ne sont pas appropriés, ils peuvent constituer des indices d'un biais possible introduit par la direction ;
- si le modèle fait l'objet d'une documentation adéquate, notamment en ce qui concerne les applications visées, les limites, les paramètres clés, les données et hypothèses requises, les résultats des validations effectuées, ainsi que la nature et le fondement des ajustements apportés aux données de sortie.

Hypothèses (Voir par. 13 (h)(ii)a.ii.)

[...]

Données (Voir par. 13 (h)(ii)a.iii.)

A44. Pour prendre connaissance de la manière dont la direction choisit les données sur lesquelles sont fondées les estimations comptables, l'auditeur peut, par exemple, prendre en considération les points suivants :

- la nature et la source des données, y compris les informations provenant de sources d'informations externes ;
- la manière dont la direction évalue si les données sont appropriées ;
- l'exactitude et l'exhaustivité des données ;
- la cohérence des données avec celles utilisées lors des périodes précédentes ;
- le degré de complexité des ~~systemes applications~~ informatiques ou d'autres aspects de l'environnement informatique servant à utilisés pour l'obtention et le au traitement des données, notamment quand le volume de données à traiter est important ;

- la manière dont les données sont obtenues, transmises et traitées et dont leur intégrité est maintenue.

Manière dont la direction acquiert une connaissance de l'incertitude d'estimation et y répond (Voir par. 13 (h)(ii)b.-c.)

[...]

~~Les activités de c-Contrôles pertinentes pour l'audit~~ identifiés qui concernent le processus d'établissement des estimations comptables par la direction (Voir par. 13 (i))

A50. C'est au processus de la direction qui est mentionné au paragraphe 13(h)(ii) que se rapporte le jugement que pose l'auditeur lorsqu'il identifie les ~~contrôles pertinents pour l'audit de la composante « mesures de contrôle »~~ et qu'il établit, par le fait même, la nécessité d'en évaluer la conception et de déterminer s'ils ont été mis en œuvre. ~~Selon la complexité de l'estimation comptable, il se peut que l'auditeur n'identifie pas de contrôles d'mesures de contrôle pertinentes pour chacun des éléments aspects~~ mentionnés au paragraphe 13 (h)(ii).

A51. ~~Pour prendre connaissance des activités de~~ Lorsqu'il identifie les contrôles pertinentes pour l'audit, évalue leur conception et détermine s'ils ont été mis en œuvre, l'auditeur peut prendre en considération :

- la manière dont la direction détermine le caractère approprié des données utilisées aux fins de l'établissement des estimations comptables, notamment quand elle a recours à une source d'informations externe ou à des données qui ne proviennent ni du grand livre ni des journaux auxiliaires ;
- l'examen et l'approbation par la direction, au niveau hiérarchique approprié, et, le cas échéant, par les personnes constituant le gouvernement d'entreprise des estimations comptables ainsi que des hypothèses et des données utilisées aux fins de leur établissement ;
- la séparation des tâches permettant d'assurer que les personnes qui ont la responsabilité d'établir les estimations comptables ne sont pas les mêmes que celles qui engagent l'entité en concluant les opérations sous-jacentes. L'auditeur se demande notamment si la nature de l'entité et de ses produits ou services a été prise en compte de façon appropriée dans la répartition des responsabilités. Par exemple, dans le cas d'une grande institution financière, une bonne façon de séparer les tâches pourrait consister à établir une fonction indépendante qui serait chargée d'établir et de valider l'estimation de la juste valeur des produits financiers de l'entité et qui serait dotée d'un personnel dont la rémunération n'est pas liée à ces produits ;
- l'efficacité de la conception des ~~contrôles mesures de contrôle~~. Il est généralement plus difficile pour la direction de concevoir des contrôles qui répondent à la subjectivité et à l'incertitude d'estimation, de façon à prévenir, ou à détecter et corriger, efficacement les anomalies significatives, que de concevoir des contrôles qui répondent à la complexité. Il se peut que les contrôles qui répondent à la subjectivité et à l'incertitude d'estimation doivent comporter davantage d'éléments manuels, lesquels sont moins fiables que les contrôles automatisés étant donné qu'il est plus facile pour la direction d'y passer outre, d'en faire abstraction ou de les contourner. L'efficacité de la conception des contrôles qui répondent à la complexité peut varier en fonction des raisons et de la nature de cette complexité. Par exemple, il peut être

plus facile de concevoir des contrôles efficaces lorsque ceux-ci se rapportent à une méthode qui est couramment utilisée ou à l'intégrité des données.

A52. Lorsque la direction a recours à l'informatique dans une large mesure pour établir une estimation comptable, il est probable que les contrôles identifiés de la composante « mesures de contrôle » pertinents pour l'audit comprennent les contrôles généraux informatiques et des contrôles ~~des applications~~ du traitement de l'information. Ces contrôles peuvent répondre aux risques liés :

- au fait que les applications informatiques ou d'autres aspects de l'environnement système informatique aient ou non la capacité de traiter d'importants volumes de données et au caractère approprié ou non de ~~sa leur~~ configuration pour cet usage ;
- aux calculs complexes que nécessite l'application d'une méthode. Lorsque plusieurs applications informatiques systèmes sont nécessaires pour le traitement d'opérations complexes, des rapprochements réguliers sont effectués entre ces applications systèmes, en particulier quand ~~les systèmes celles-ci~~ n'ont pas d'interfaces automatisées ou qu'~~ils elles~~ sont susceptibles de faire l'objet d'interventions manuelles ;
- au fait que la conception et le calibrage des modèles font ou non l'objet d'évaluations périodiques ;
- à l'exhaustivité et à l'exactitude de l'extraction des données relatives aux estimations comptables des comptes de l'entité ou de sources d'informations externes ;
- aux données, ce qui comprend l'exhaustivité et l'exactitude du flux des données transitant par le système d'information de l'entité, le caractère approprié de toute modification des données utilisées aux fins de l'établissement des estimations comptables, ainsi que le maintien de l'intégrité et de la sécurité des données ;
- au traitement ou à l'enregistrement des données, lorsque la direction a recours à des sources d'informations externes ;
- au fait que la direction s'est dotée ou non de contrôles sur l'accès aux différents modèles, leur modification et leur maintenance, afin de conserver une piste d'audit fiable pour les versions approuvées des modèles et d'empêcher qu'on puisse accéder à ces modèles ou les modifier sans autorisation ;
- à la présence ou à l'absence de contrôles appropriés à l'égard du transfert d'informations relatives aux estimations comptables dans le grand livre, notamment sur les écritures comptables.

A53. Dans certains secteurs, comme ceux des banques et de l'assurance, il se peut que le terme « gouvernance » soit employé pour décrire des activités faisant partie de l'environnement de contrôle, du processus de suivi du système de contrôle interne par l'entité ~~suivi des contrôles~~ ou d'autres composantes du système de contrôle interne, qui sont décrites dans la norme ISA 315 (révisée en 2019)¹³⁵.

¹³⁵ Norme ISA 315 (révisée en 2019), paragraphe A77Annexe 3.

A54. Lorsque l'entité dispose d'une fonction d'audit interne, les travaux de celle-ci peuvent être particulièrement utiles à l'auditeur. En effet, ces travaux peuvent l'aider à prendre connaissance :

- de la nature et de l'étendue de l'utilisation des estimations comptables par la direction ;
- de la conception et de la mise en œuvre des contrôles ~~mesures de contrôle~~ visant à répondre aux risques liés aux données, aux hypothèses et aux modèles servant à établir les estimations comptables ;
- des aspects du système d'information de l'entité qui génère les données sur lesquelles sont fondées les estimations comptables ;
- de la manière dont les nouveaux risques liés aux estimations comptables sont identifiés, évalués et gérés.

Examen du dénouement ou de la révision d'estimations comptables antérieures (Voir par. 14)

[...]

A58. Selon l'évaluation antérieure qu'a faite l'auditeur des risques d'anomalies significatives, par exemple s'il détermine que le risque inhérent est plus élevé en ce qui a trait à un ou à plusieurs risques d'anomalies significatives, il peut juger nécessaire de procéder à un examen rétrospectif plus détaillé. Dans le cadre d'un tel examen, l'auditeur pourra, par exemple, porter une attention particulière – dans la mesure où cela est faisable en pratique – à l'incidence des hypothèses importantes et des données qui ont servi à établir les estimations comptables antérieures. À l'inverse, pour les estimations comptables découlant de l'enregistrement d'opérations courantes et récurrentes, par exemple, l'auditeur peut juger que les procédures d'évaluation des risques mises en œuvre aux fins de l'examen peuvent se limiter à des procédures analytiques.

A59. L'objectif d'évaluation, en ce qui concerne les estimations comptables en juste valeur et d'autres estimations comptables – qui sont fondées sur les conditions existant à la date d'évaluation –, implique des perceptions de valeur à un moment précis, perceptions qui peuvent changer considérablement et rapidement selon l'évolution de l'environnement dans lequel l'entité exerce ses activités. C'est pourquoi l'auditeur peut orienter l'examen de manière à obtenir des informations pertinentes pour l'identification et l'évaluation des risques d'anomalies significatives. Par exemple, dans certains cas, il se peut que la connaissance des changements dans les hypothèses des intervenants du marché qui ont eu une incidence sur le dénouement d'estimations comptables en juste valeur d'une période précédente ait peu de chances de fournir des éléments probants pertinents. En pareils cas, des éléments probants peuvent être recueillis par la prise de connaissance du dénouement des hypothèses (par exemple des projections des flux de trésorerie) et de l'efficacité du processus d'estimation suivi par la direction dans le passé, éléments probants qui étayeront l'identification et l'évaluation des risques d'anomalies significatives relatifs à la période en cours.

A60. Un écart entre une estimation comptable comptabilisée dans les états financiers de la période précédente et son dénouement n'est pas nécessairement un indice d'anomalie dans les états financiers de la période précédente. Toutefois, un tel écart peut indiquer une anomalie si, par exemple, il découle du fait que la direction n'a pas tenu compte d'informations dont elle disposait au moment de la finalisation des états financiers de la période précédente ou dont on pouvait raisonnablement s'attendre à ce qu'elles soient obtenues et prises en considération par la direction

au regard du référentiel comptable applicable¹³⁶. Un tel écart peut remettre en cause le processus suivi par la direction pour la prise en considération des informations aux fins de l'établissement des estimations comptables. En conséquence, l'auditeur peut réévaluer les tests prévus des contrôles connexes, le cas échéant, et l'évaluation du le risque lié au contrôle interne s'y rapportant et ou déterminer que des éléments probants plus convaincants doivent être recueillis quant à cette question. De nombreux référentiels d'information financière donnent des indications sur la manière de distinguer, parmi les changements dans les estimations comptables, ceux qui constituent des anomalies et ceux qui n'en constituent pas, ainsi que sur le traitement comptable à appliquer dans chaque cas.

Compétences ou connaissances spécialisées (Voir par. 15)

[...]

Identification et évaluation des risques d'anomalies significatives (Voir par. 4, 16)

A64. Il importe de procéder à l'identification et à l'évaluation des risques d'anomalies significatives au niveau des assertions liées aux estimations comptables pour toutes les estimations comptables, c'est-à-dire non seulement pour celles qui sont comptabilisées dans les états financiers, mais aussi pour celles incluses dans les notes des états financiers.

A65. Selon le paragraphe A42 de la norme ISA 200, les normes ISA se réfèrent généralement aux « risques d'anomalies significatives » et le risque inhérent et le risque lié au contrôle interne ne sont pas traités séparément. ~~Toutefois, la présente~~ La norme ISA 315 (révisée en 2019) requiert une évaluation séparée du risque inhérent et du risque lié au contrôle interne afin d'établir une base pour la conception et la mise en œuvre de procédures d'audit complémentaires en réponse aux risques d'anomalies significatives au niveau des assertions¹³⁷, y compris les risques importants, ~~qui sont liés aux estimations comptables~~, conformément à la norme ISA 330¹³⁸.

A66. Pour identifier les risques d'anomalies significatives et évaluer le risque inhérent lié aux estimations comptables selon la norme ISA 315 (révisée en 2019)¹³⁹, l'auditeur doit tenir compte ~~de la mesure dans laquelle l'estimation comptable est touchée par des facteurs de risque inhérent ayant une incidence sur la possibilité que les assertions comportent des anomalies, et de la façon dont ils influent sur cette possibilité~~ l'incertitude d'estimation, la complexité, la subjectivité ou d'autres facteurs de risque inhérent. La prise en considération des facteurs de risque inhérent peut aussi permettre à l'auditeur d'obtenir des informations qui lui serviront :

- à évaluer la probabilité et l'ampleur d'une anomalie (c.-à-d. à situer l'évaluation du risque inhérent sur l'échelle de risque inhérent) ;
- à cerner les raisons qui sous-tendent l'évaluation des risques d'anomalies significatives au niveau des assertions, et à s'assurer que les procédures d'audit complémentaires qu'il met en œuvre conformément au paragraphe 18 sont adaptées à ces raisons.

¹³⁶ Norme ISA 560, *Événements postérieurs à la date de clôture*, paragraphe 14.

¹³⁷ Norme ISA 315 (révisée en 2019), paragraphes 31 et 34.

¹³⁸ Norme ISA 330, par. 7 (b).

¹³⁹ Norme ISA 315 (révisée en 2019), par. 31 (a).

Les interrelations entre les facteurs de risque inhérent sont expliquées de façon plus détaillée à l'Annexe 1.

- A67. Les raisons qui sous-tendent l'évaluation par l'auditeur du risque inhérent au niveau des assertions peuvent être attribuables à un seul ou à plusieurs facteurs de risque inhérent – incertitude d'estimation, complexité, subjectivité ou autres. Par exemple :
- (a) les estimations comptables des pertes de crédit attendues seront probablement complexes, car ces pertes ne sont pas directement observables et doivent souvent être estimées au moyen d'un modèle complexe. Le modèle peut reposer sur un ensemble complexe de données historiques et d'hypothèses au sujet d'événements futurs liés à divers scénarios propres à l'entité qui peuvent être difficiles à prédire. Il est également probable que les estimations comptables des pertes de crédit attendues comportent un degré élevé d'incertitude d'estimation et qu'elles présentent une part importante de subjectivité, du fait qu'elles nécessitent de porter des jugements à l'égard des événements ou situations futurs. Des considérations similaires s'appliquent aux passifs d'assurance ;
 - (b) l'estimation comptable d'une provision pour obsolescence des stocks d'une entité ayant un large éventail de stocks peut, selon la nature des stocks, nécessiter des systèmes et des processus complexes, mais comporter de faibles degrés de subjectivité et d'incertitude d'estimation ;
 - (c) des estimations comptables peuvent ne pas être complexes, mais comporter un degré élevé d'incertitude d'estimation et requérir une grande part de jugement, comme c'est le cas, par exemple, d'une estimation comptable qui requiert un jugement critique à l'égard d'un passif dont le montant dépend de l'issue d'un procès.
- A68. La pertinence et l'importance des facteurs de risque inhérent peuvent varier d'une estimation à l'autre. Par conséquent, il est possible que les facteurs de risque inhérent, seuls ou en association avec d'autres, aient une incidence moindre sur les estimations comptables simples, et que l'auditeur identifie moins de risques ou évalue que le risque inhérent se ~~situe dans~~ rapproche de la partie inférieure de l'échelle de risque inhérent.
- A69. À l'inverse, il est possible que les facteurs de risque inhérent, seuls ou en association avec d'autres, aient une incidence accrue sur les estimations comptables complexes, et que l'auditeur évalue que le risque inhérent se situe dans la partie supérieure de l'échelle de risque inhérent. Il est alors probable que la prise en considération par l'auditeur de l'incidence des facteurs de risque inhérent aura un effet direct sur le nombre et la nature des risques d'anomalies significatives identifiés, sur l'évaluation de ces risques, et ultimement sur le caractère convaincant des éléments probants à recueillir pour répondre à l'évaluation des risques. De plus, il se peut que l'exercice de l'esprit critique par l'auditeur soit particulièrement important dans le cas de ces estimations comptables.
- A70. Des événements survenus après la date de clôture peuvent fournir des informations supplémentaires pertinentes pour l'évaluation par l'auditeur des risques d'anomalies significatives au niveau des assertions. Par exemple, il se peut qu'on prenne connaissance du dénouement d'une estimation comptable au cours de l'audit. Cela peut amener l'auditeur à évaluer ou à réévaluer les risques

d'anomalies significatives au niveau des assertions¹⁴⁰, et ce, indépendamment de la façon dont les facteurs de risque inhérent influent sur la possibilité que les assertions relatives à l'estimation comptable comportent des anomalies ~~mesure dans laquelle l'estimation comptable était touchée par l'incertitude d'estimation, la complexité, la subjectivité ou d'autres facteurs de risque inhérent~~. Les événements survenus après la date de clôture peuvent aussi influencer sur l'approche que l'auditeur choisit pour tester l'estimation comptable conformément au paragraphe 18. Par exemple, pour une simple prime à payer à certains employés en fonction d'un pourcentage de leur rémunération, l'auditeur peut conclure que la complexité ou la part de subjectivité que comporte l'établissement de l'estimation comptable sont relativement faibles, et donc évaluer que le risque inhérent au niveau des assertions se ~~situe dans~~ rapproche de la partie inférieure de l'échelle de risque inhérent. Le versement des primes après la fin de la période peut fournir des éléments probants suffisants et appropriés pour l'évaluation des risques d'anomalies significatives au niveau des assertions.

- A71. L'auditeur peut procéder à l'évaluation du risque lié au contrôle interne de diverses façons, en fonction des techniques ou des méthodes d'audit qu'il privilégie. Le résultat de l'évaluation du risque lié au contrôle interne peut être exprimé à l'aide de catégories qualitatives (par exemple, risque lié au contrôle interne maximal, modéré ou minimal) ou en fonction des attentes de l'auditeur en ce qui concerne l'efficacité avec laquelle les contrôles répondent au risque identifié, c'est-à-dire, de son intention de s'appuyer sur l'efficacité du fonctionnement des contrôles. Par exemple, si le risque lié au contrôle interne est établi au maximum, l'auditeur n'envisage pas de s'appuyer sur l'efficacité du fonctionnement des contrôles, mais il envisage de le faire s'il établit le risque lié au contrôle interne à un niveau inférieur au maximum.

Incertitude d'estimation (Voir par. 16(a))

- A72. Pour tenir compte du degré d'incertitude d'estimation que comportent les estimations comptables, l'auditeur peut prendre en considération :
- le fait que le référentiel comptable applicable requiert ou non :
 - le recours, pour l'établissement des estimations comptables, à une méthode d'estimation qui comporte de façon inhérente un degré élevé d'incertitude d'estimation. Par exemple, un référentiel d'information financière peut requiert l'utilisation de données d'entrée non observables,
 - l'utilisation d'hypothèses qui comportent de façon inhérente un degré élevé d'incertitude d'estimation, telles que des hypothèses à long terme, l'utilisation d'hypothèses qui sont basées sur des données non observables et que la direction peut donc difficilement établir, ou l'utilisation de diverses hypothèses interreliées,
 - la fourniture d'informations sur l'incertitude d'estimation ;
 - le contexte commercial. Il peut arriver que le marché dans lequel l'entité exerce ses activités traverse une période de turbulences ou de stagnation (en raison, par exemple, de fluctuations importantes des taux de change ou du ralentissement des marchés) et que les estimations comptables soient donc basées sur des données difficilement observables ;

¹⁴⁰ Norme ISA 315 (révisée en 2019), paragraphe 3734.

- la possibilité (ou la faisabilité en pratique, dans la mesure où le référentiel comptable applicable le permet) pour la direction :
 - de prédire, avec précision et fiabilité, la valeur qui sera réalisée au titre d'une opération passée (par exemple, le montant qui sera payé en vertu d'une clause conditionnelle), ou les incidences d'événements ou de situations futurs (par exemple, le montant d'une perte de crédit future, ou le montant et le moment du règlement d'une demande d'indemnisation),
 - d'obtenir des informations précises et complètes concernant une situation actuelle (par exemple, des informations sur les variables d'évaluation permettant de simuler le point de vue des intervenants du marché à la date de clôture aux fins de l'établissement d'estimations en juste valeur).

A73. Le fait que le montant comptabilisé ou fourni à titre d'information dans les états financiers relativement à une estimation comptable soit faible ou élevé n'est pas en soi un bon indice de la possibilité que cette estimation comporte une anomalie, parce qu'il peut y avoir eu sous-évaluation, par exemple.

A74. Dans certaines circonstances, le degré d'incertitude d'estimation peut être si élevé qu'il est impossible d'établir une estimation comptable raisonnable. Le référentiel comptable applicable peut alors interdire la comptabilisation d'un élément dans les états financiers ou son évaluation à la juste valeur. Dans de tels cas, il peut y avoir des risques d'anomalies significatives liés non seulement à la question de savoir s'il faut comptabiliser l'estimation comptable ou s'il faut l'évaluer à la juste valeur, mais aussi à celle de savoir si les informations fournies sont raisonnables. Le référentiel comptable applicable peut requérir la fourniture d'informations sur les estimations comptables de ce type et sur l'incertitude d'estimation qui leur est associée (voir par. A112–A113, A143– A144).

A75. Dans certains cas, l'incertitude d'estimation d'une estimation comptable peut jeter un doute important sur la capacité de l'entité à poursuivre son exploitation. La norme ISA 570 (révisée)¹⁴¹ définit des diligences et fournit des indications à ce sujet.

Complexité ou subjectivité (Voir par. 16(b))

Mesure dans laquelle la complexité a une incidence sur le choix et l'application de la méthode

A76. Pour tenir compte de la mesure dans laquelle le choix et l'application de la méthode utilisée pour l'établissement des estimations comptables sont touchés par la complexité, l'auditeur peut prendre en considération :

- les besoins de la direction en matière de compétences ou de connaissances spécialisées, qui peuvent indiquer que la méthode utilisée pour l'établissement des estimations comptables comporte une complexité inhérente et donc que ces estimations sont plus sujettes aux anomalies significatives. Il se peut que la possibilité que les estimations comportent des anomalies significatives soit plus grande lorsque la direction a mis au point en interne un

¹⁴¹ Norme ISA 570 (révisée), *Continuité de l'exploitation*.

modèle et qu'elle possède relativement peu d'expérience dans ce domaine, ou qu'elle a recours à un modèle pour appliquer une méthode qui n'est pas bien connue ni communément utilisée dans le secteur d'activité ou l'environnement particulier concerné ;

- la nature de la base d'évaluation prescrite par le référentiel comptable applicable, qui peut nécessiter le recours à une méthode complexe faisant appel à différentes sources de données historiques et prospectives ou à plusieurs hypothèses prévisionnelles ayant de multiples interrelations. Par exemple, lorsqu'on établit une provision pour pertes de crédit attendues, il peut être nécessaire de se fonder sur des données empiriques historiques et des hypothèses prévisionnelles pour porter des jugements sur des créances qu'on prévoit recouvrer et d'autres flux de trésorerie attendus. De même, l'évaluation d'un passif d'assurance peut requérir qu'on se fonde sur des données empiriques historiques et des tendances actuelles et prévisionnelles pour porter des jugements sur les paiements prévus au titre d'un contrat d'assurance.

Mesure dans laquelle la complexité a une incidence sur le choix et l'application des données

A77. Pour tenir compte de la mesure dans laquelle le choix et l'application des données utilisées pour l'établissement des estimations comptables sont touchés par la complexité, l'auditeur peut prendre en considération :

- la complexité du processus par lequel les données sont générées, ainsi que la pertinence et la fiabilité de la source des données. La fiabilité des données peut varier d'une source à l'autre. De plus, pour des raisons de confidentialité ou d'exclusivité, les informations permettant d'évaluer la fiabilité des données fournies, comme l'origine des données sous-jacentes utilisées ou la façon dont celles-ci ont été recueillies et traitées, ne sont pas toujours communiquées, du moins pas en totalité, par les sources externes ;
- la complexité inhérente au maintien de l'intégrité des données. Il peut y avoir une telle complexité lorsque les données utilisées aux fins de l'établissement des estimations comptables sont volumineuses et proviennent de multiples sources ;
- la nécessité d'interpréter des modalités contractuelles complexes. Par exemple, la détermination des entrées ou sorties de trésorerie liées aux remises accordées par des fournisseurs ou à des clients peut dépendre de modalités contractuelles très complexes dont la connaissance ou l'interprétation nécessitent une expérience ou des compétences particulières.

Mesure dans laquelle la subjectivité a une incidence sur le choix et l'application de la méthode, des hypothèses ou des données

A78. Pour tenir compte de la mesure dans laquelle le choix et l'application de la méthode, des hypothèses ou des données sont touchés par la subjectivité, l'auditeur peut prendre en considération :

- la mesure dans laquelle le référentiel comptable applicable précise – ou le fait qu'il ne précise pas – les approches, concepts, techniques et facteurs d'évaluation sur lesquels baser la méthode d'estimation ;
- l'incertitude relative aux montants ou au calendrier, notamment la durée de l'horizon prévisionnel. En raison de l'incertitude d'estimation inhérente aux montants et au calendrier, la direction est appelée à exercer son jugement pour choisir une estimation ponctuelle ; il se

peut alors qu'elle introduise des biais. Ainsi, une estimation comptable qui intègre des hypothèses prévisionnelles peut comporter un degré élevé de subjectivité et est donc vulnérable à un biais introduit par la direction.

Autres facteurs de risque inhérent (Voir par. 16(b))

A79. Le degré de subjectivité associé à une estimation comptable peut influencer sur la vulnérabilité de celle-ci aux anomalies résultant de partis pris de la direction ou d'autres facteurs de risque de fraudes, dans la mesure où ils influent sur le risque inhérent. Par exemple, une estimation comptable comportant un degré élevé de subjectivité sera probablement plus vulnérable aux anomalies résultant de partis pris de la direction ou de fraudes. En effet, il se pourrait que l'évaluation aboutisse à une large fourchette de résultats possibles, et que la direction choisisse, à l'intérieur de cette fourchette, une estimation ponctuelle qui est inappropriée dans les circonstances ou qui est influencée indûment par un biais volontaire ou involontaire de sa part, ce qui donnerait lieu à une anomalie. Dans le cas d'audits récurrents, les indices d'un biais possible de la direction détectés au cours des audits des périodes précédentes peuvent influencer sur la planification et sur les procédures d'évaluation des risques pour la période en cours.

Risques importants (Voir par. 17)

A80. L'évaluation que fait l'auditeur du risque inhérent, en tenant compte de la mesure dans laquelle l'estimation comptable est touchée par l'incertitude d'estimation, la complexité, la subjectivité ou d'autres facteurs de risque inhérent, l'aide à déterminer s'il y a des risques importants parmi les risques d'anomalies significatives identifiés et évalués.

[...]

Cas où l'auditeur a l'intention de s'appuyer sur l'efficacité du fonctionnement des contrôles pertinents (Voir par. 19)

A85. Il peut être approprié de tester l'efficacité du fonctionnement des contrôles ~~pertinents~~, notamment en ce qui concerne les risques importants, lorsque l'évaluation du risque inhérent se situe dans la partie supérieure de l'échelle de risque inhérent, comme ce peut être le cas lorsque l'estimation comptable est touchée par un degré élevé de complexité. Lorsque l'estimation comptable comporte un degré élevé de subjectivité, et donc qu'elle fait largement appel au jugement de la direction, les limites inhérentes à l'efficacité de la conception des contrôles peuvent mener l'auditeur à mettre davantage l'accent sur les contrôles de substance que sur les tests de l'efficacité du fonctionnement des contrôles.

[...]

Évaluation globale fondée sur les procédures d'audit réalisées (Voir par. 33)

[...]

Évaluation visant à déterminer si les estimations comptables sont raisonnables ou si elles comportent des anomalies (Voir par. 9, 35)

[...]

Norme ISA 600, Audits d'états financiers de groupe (y compris l'utilisation des travaux des auditeurs des composantes) — Considérations particulières

Diligences

[...]

Connaissance du groupe, de ses composantes et de leurs environnements

17. L'auditeur est tenu d'identifier et d'évaluer les risques d'anomalies significatives en acquérant une connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité⁷. L'équipe affectée à l'audit du groupe doit :

(a) [...]

Modalités d'application et autres commentaires explicatifs

[...]

Définitions

[...]

Composante importante (Voir par. 9 (m))

[...]

A6. L'équipe affectée à l'audit du groupe peut également déterminer qu'il est probable qu'une composante soit, en raison de sa nature ou des circonstances qui lui sont propres, à l'origine de risques importants d'anomalies significatives dans les états financiers de groupe ~~(c'est-à-dire des risques exigeant une attention particulière dans le cadre de la mission~~¹⁴²). Par exemple, une composante peut être chargée des opérations de change et ainsi exposer le groupe à un risque important d'anomalies significatives, même si, par ailleurs, elle n'est pas importante sur le plan financier lorsque prise isolément.

[...]

Connaissance du groupe, de ses composantes et de leurs environnements

Éléments dont l'équipe affectée à l'audit du groupe acquiert une connaissance (Voir par. 17)

A23. La norme ISA 315 (révisée en 2019) contient des indications sur les éléments dont l'auditeur peut tenir compte lorsqu'il acquiert une connaissance : des facteurs sectoriels et réglementaires, ainsi que des autres facteurs externes ayant une incidence sur l'entité, y compris le référentiel comptable applicable ; de la nature de l'entité ; de ses objectifs et stratégies et des risques liés à l'activité connexes ; de la mesure et de l'analyse de la performance financière de l'entité¹⁴³. L'Annexe 2 de la

¹⁴² Norme ISA 315 (révisée), paragraphes 27-29.

¹⁴³ Norme ISA 315 (révisée en 2019), paragraphes A25-A62 à A49A64 et Annexe 1.

présente norme ISA contient des indications sur les éléments propres aux groupes, y compris le processus de consolidation.

Annexe 2
(Voir par. A23)

Exemples d'éléments dont l'équipe affectée à l'audit du groupe acquiert une connaissance

[...]

Contrôles à l'échelle du groupe

1. Les contrôles à l'échelle du groupe peuvent être constitués d'une combinaison des éléments suivants :
 - réunions courantes entre la direction du groupe et la direction des composantes pour traiter de l'évolution des affaires et pour passer en revue les performances ;
 - [...]
 - ~~mesures de contrôle~~ contrôles intégrées à un système informatique commun à toutes les composantes ou à certaines d'entre elles ;
 - ~~suivi des~~ contrôles qui font partie du processus de suivi du système de contrôle interne par le groupe, ce qui comprend les activités de la fonction d'audit interne et les programmes d'autoévaluation ;
 - [...]

Annexe 5
(Voir par. A58)

Éléments obligatoires et complémentaires du contenu de la lettre d'instructions de l'équipe affectée à l'audit du groupe

[...]

Questions liées à la planification des travaux de l'auditeur de la composante :

- [...]

Questions liées à la réalisation des travaux de l'auditeur de la composante :

- les constatations de l'équipe affectée à l'audit du groupe à la suite des tests de procédures qu'elle a effectués sur un système de traitement commun à tout ou partie des composantes, et les tests de procédures à effectuer par l'auditeur de la composante ;
- [...]

Norme ISA 610 (révisée en 2013), *Utilisation des travaux des auditeurs internes*

Introduction

[...]

Relation entre la norme ISA 315 (révisée en 2019) et la norme ISA 610 (révisée en 2013)

[...]

7. La norme ISA 315 (révisée en 2019) traite de la façon dont les connaissances et l'expérience de la fonction d'audit interne peuvent aider l'auditeur externe à prendre connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité, ainsi qu'à identifier et à évaluer les risques d'anomalies significatives. La norme ISA 315 (révisée en 2019)³ explique également en quoi une communication efficace entre les auditeurs internes et externes crée aussi un environnement qui permet à l'auditeur externe de prendre connaissance de questions importantes susceptibles d'avoir une incidence sur ses travaux.

[...]

Modalités d'application et autres commentaires explicatifs

Définition de « fonction d'audit interne » (Voir par. 2 et par. 14 (a))

[...]

- A3. De plus, en raison des menaces pour l'objectivité auxquelles font face les personnes assumant des fonctions et des responsabilités liées à l'exploitation et à la gestion qui sont extérieures à la fonction d'audit interne de l'entité, ces personnes ne peuvent être considérées comme faisant partie d'une fonction d'audit interne aux fins de la présente norme ISA, même si elles sont susceptibles de mettre en œuvre ~~réaliser des mesures de contrôle~~ contrôles pouvant faire l'objet de tests conformément à la norme ISA 330¹². C'est pourquoi les contrôles de surveillance mis en œuvre par un propriétaire-dirigeant ne sont pas considérés comme étant l'équivalent d'une fonction d'audit interne.

[...]

Évaluation de la fonction d'audit interne

[...]

Adoption d'une approche systématique et rigoureuse (Voir par. 15 (c))

- A10. L'adoption par la fonction d'audit interne d'une approche systématique et rigoureuse à l'égard de la planification, de la réalisation, de la supervision, de la revue et de la documentation de ses activités permet de distinguer celles-ci des autres ~~mesures de contrôles~~ de suivi réalisées ~~mis en œuvre~~ au sein de l'entité.

[...]

A21. Comme il est expliqué dans la norme ISA 315 (révisée en 2019)¹⁴⁴, les risques importants sont ceux qui, selon l'évaluation de l'auditeur, se situent près de l'extrémité supérieure de l'échelle de risque inhérent exigent une attention spéciale sur le plan de l'audit et. Par conséquent, les possibilités d'utilisation des travaux de la fonction d'audit interne en cas de risques importants se limiteront aux résultats des procédures faisant appel à une part limitée de jugement. De plus, lorsque le risque d'anomalies significatives est autre que faible, il est peu probable que la seule utilisation des travaux de la fonction d'audit interne permette de ramener le risque d'audit à un niveau acceptable et d'éliminer la nécessité, pour l'auditeur externe, de mettre en œuvre lui-même certains tests.

[...]

Norme ISA 620, *Utilisation par l'auditeur des travaux d'un expert de son choix*

Modalités d'application et autres commentaires explicatifs

[...]

Détermination de la nécessité pour l'auditeur de faire appel à un expert de son choix (Voir par. 7)

A4. L'auditeur peut juger nécessaire de faire appel à un expert pour l'assister dans ses travaux en ce qui concerne l'un ou plusieurs des aspects suivants :

- la prise de connaissance de l'entité et de son environnement, ~~y compris son~~ du référentiel comptable applicable et du système de contrôle interne de l'entité ;
- [...]

Norme ISA 701, *Communication des questions clés de l'audit dans le rapport de l'auditeur indépendant*

Modalités d'application et autres commentaires explicatifs

[...]

Détermination des questions clés de l'audit (Voir par. 9 et 10)

[...]

Points à prendre en considération dans la détermination des questions ayant nécessité une attention importante de la part de l'auditeur (Voir par. 9)

[...]

Aspects considérés comme présentant des risques d'anomalies significatives élevés ou à l'égard desquels des risques importants ont été identifiés conformément à la norme ISA 315 (révisée en 2019) (Voir par. 9 (a))

[...]

¹⁴⁴ Norme ISA 315 (révisée en 2019), par. 12 (l)-4 e).

A20. Selon la norme ISA 315 (révisée en 2019), un risque important s'entend d'un risque d'anomalies significatives identifié pour lequel l'évaluation du risque inhérent se situe près de l'extrémité supérieure de l'échelle de risque inhérent en raison de la mesure dans laquelle les facteurs de risque inhérent influent sur la combinaison que forment la probabilité qu'une anomalie se produise et l'ampleur qu'elle pourrait prendre, le cas échéant et évalué qui, selon le jugement de l'auditeur, exige une attention importante dans le cadre de la mission¹⁴⁵. Les aspects à l'égard desquels la direction doit porter des jugements importants et les opérations inhabituelles importantes peuvent souvent être identifiés comme des risques importants. Il est donc fréquent que les risques importants constituent des aspects nécessitant une attention importante de la part de l'auditeur.

[...]

Norme ISA 720 (révisée), Responsabilités de l'auditeur concernant les autres informations

Modalités d'application et autres commentaires explicatifs

[...]

Lecture et prise en considération des autres informations (Voir par. 14–15)

[...]

Appréciation quant à l'existence d'une incohérence significative entre les autres informations et la connaissance acquise par l'auditeur au cours de l'audit (Voir par. 14 (b))

[...]

A31. La connaissance acquise par l'auditeur au cours de l'audit englobe la connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système y compris de son contrôle interne de l'entité, acquise conformément à la norme ISA 315 (révisée en 2019)¹⁴⁶. La norme ISA 315 (révisée en 2019) fait état de la connaissance qui doit être acquise par l'auditeur, laquelle implique notamment la prise de connaissance des éléments suivants :

- (a) la structure organisationnelle de l'entité, son actionnariat et sa structure de gouvernance ainsi que son modèle économique, dont la mesure dans laquelle le recours à l'informatique y est intégré ;
- (b) les facteurs sectoriels, ~~et les facteurs~~ réglementaires, ~~ainsi que et~~ les autres facteurs externes pertinents ;
- (c) les mesures pertinentes qui sont utilisées par l'entité ou par des parties externes aux fins de l'évaluation et l'analyse de la performance financière de l'entité ;
- (b) ~~la nature de l'entité ;~~
- (c) ~~le choix et l'application des méthodes comptables retenues par l'entité ;~~
- (d) ~~les objectifs et les stratégies de l'entité ;~~

¹⁴⁵ Norme ISA 315 (révisée en 2019), par. 12 (l)

¹⁴⁶ Norme ISA 315 (révisée en 2019), *Compréhension de l'entité et de son environnement aux fins de l'identification et de l'évaluation des risques d'anomalies significatives*, paragraphes 44 et 42-19-27.

[...]

Réponse lorsqu'il existe une anomalie significative dans les états financiers ou que l'auditeur doit mettre à jour sa connaissance de l'entité et de son environnement (Voir par. 20)

A51. Lorsque l'auditeur lit les autres informations, il se peut qu'il prenne connaissance de nouvelles informations qui ont des conséquences sur :

- sa connaissance de l'entité et de son environnement, du référentiel comptable applicable et du système de contrôle interne de l'entité, ce qui peut indiquer la nécessité de revoir l'évaluation qu'il a faite des risques ;
- [...]

[...]

L'IAASB dispose des structures et des processus nécessaires à l'exercice de ses activités grâce au concours de l'*International Federation of Accountants*[®] (IFAC[®]).

L'IAASB et l'IFAC déclinent toute responsabilité en cas de préjudice subi par toute personne qui agit ou s'abstient d'agir en se fiant à la présente publication, que ledit préjudice soit attribuable à une faute ou à une autre cause.

Les *International Standards on Auditing*, les *International Standards on Assurance Engagements*, les *International Standards on Review Engagements*, les *International Standards on Related Services*, les *International Standards on Quality Control*, les *International Auditing Practice Notes*, les exposés-sondages, les documents de consultation et autres publications de l'IAASB sont publiés par l'IFAC, qui est titulaire des droits d'auteur s'y rattachant.

Copyright © Décembre 2019 IFAC. Tous droits réservés. Le présent document peut être téléchargé à des fins personnelles et non commerciales (pour les besoins de consultation à titre professionnel ou de recherche) à l'adresse www.iaasb.org. Il est nécessaire d'obtenir une autorisation écrite pour la traduction, la reproduction, le stockage ou la transmission de ce document, ou son utilisation à d'autres fins similaires.

Les appellations « *International Auditing and Assurance Standards Board* », « *International Standards on Auditing* », « *International Standards on Assurance Engagements* », « *International Standards on Review Engagements* », « *International Standards on Related Services* », « *International Standards on Quality Control* », « *International Auditing Practice Notes* », les sigles « IAASB », « ISA », « ISAE », « ISRE », « ISRS », « ISQC », « IAPN », ainsi que le logo de l'IAASB sont des marques de commerce ou des marques de commerce et de service déposées de l'IFAC, aux États-Unis et dans d'autres pays.

Pour obtenir des renseignements sur les droits d'auteur, les marques de commerce et les permissions, veuillez consulter le [site Web](#) (en anglais) de l'IFAC ou écrire à permissions@ifac.org.

La présente prise de position définitive, *Norme ISA 315 (révisée en 2019) et modifications de concordance et modifications corrélatives apportées à d'autres normes internationales par suite de la publication de la norme ISA 315 (révisée en 2019)*, publiée en anglais par l'IFAC en décembre 2019, a été traduite en français par Comptables professionnels agréés du Canada / Chartered Professional Accountants of Canada (CPA Canada) en mars 2020, et est utilisée avec la permission de l'IFAC. Le processus suivi pour la traduction de la prise de position définitive *Norme ISA 315 (révisée en 2019) et modifications de concordance et modifications corrélatives apportées à d'autres normes internationales par suite de la publication de la norme ISA 315 (révisée en 2019)* a été examiné par l'IFAC, et la traduction a été effectuée conformément au *Policy Statement de l'IFAC – Policy for Translating and Reproducing Standards*. La version approuvée de la prise de position définitive *Norme ISA 315 (révisée en 2019) et modifications de concordance et modifications corrélatives apportées à d'autres normes internationales par suite de la publication de la norme ISA 315 (révisée en 2019)* est celle qui est publiée en langue anglaise par l'IFAC. L'IFAC décline toute responsabilité quant à l'exactitude et à l'exhaustivité de cette traduction française, ou aux actions qui pourraient découler de son utilisation.

Texte anglais de la prise de position définitive *Norme ISA 315 (révisée en 2019) et modifications de concordance et modifications corrélatives apportées à d'autres normes internationales par suite de la publication de la norme ISA 315 (révisée en 2019)* © 2019 par l'International Federation of Accountants (IFAC). Tous droits réservés.

Texte français de la prise de position définitive *Norme ISA 315 (révisée en 2019) et modifications de concordance et modifications corrélatives apportées à d'autres normes internationales par suite de la*

publication de la norme ISA 315 (révisée en 2019) © 2022 par l'International Federation of Accountants (IFAC). Tous droits réservés.

Titre original : ISA 315 (Revised 2019) and Conforming and Consequential Amendments to Other International Standards Arising from ISA 315 (Revised 2019)



**International Auditing
and Assurance
Standards Board**

529 Fifth Avenue, New York, NY 10017
T + 1 (212) 286-9344 F +1 (212) 286-9570
www.iaasb.org