Prise de position définitive
Décembre 2019

Norme internationale d'audit 315 (révisée en 2019)

ISA 315 (révisée en 2019)

Identification et évaluation des risques d'anomalies significatives

IAASB
International Auditing and Assurance Standards Board

À propos de l'IAASB

La présente Norme internationale d'audit (ISA) de l'*International Auditing and Assurance Standards Board* (IAASB) publiée en anglais par l'*International Federation of Accountants* (IFAC) en 2022, a été traduite en français par l'Institut des Réviseurs d'Entreprises (IRE) de Belgique, la Compagnie Nationale des Commissaires aux Comptes (CNCC) et le Conseil supérieur de l'Ordre des Experts-Comptables (CSOEC) de France en 2022, et est reproduite avec la permission de l'IFAC. Le processus suivi pour la traduction des Normes internationales d'audit (ISA) 315 (révisée 2019) a été examiné par l'IFAC et la traduction a été effectuée conformément au « *Policy Statement- Policy for Translating and Reproducing Standards published by IFAC ».* La version approuvée de la Norme internationale d'audit (ISA) 315 (révisée 2019) est celle qui est publiée en langue anglaise par l'IFAC.

Titre original : *International Standard on Auditing 315 (Revised 2019), Identifying and Assessing the Risks of Material Misstatement.*

Source originale : *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2022 Edition Volume I* - ISBN number: 978-1-60815-546-0.

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

Source originale : *Handbook of International Quality Management, Review, Other Assurance, and Related Services Pronouncements, 2022 Edition Volume I*

Annexe 6 : Eléments 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 financiers[1], dont celui qui consiste à recueillir des éléments probants suffisants et appropriés pour réduire le risque d'audit à un niveau suffisamment faible[2]. Le risque d'audit est fonction des risques d'anomalies significatives et du risque de non-détection[3]. La norme ISA 200 précise que les risques d'anomalies significatives peuvent se situer à deux niveaux[4] : 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 significatives[5].

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 appropriés[6]. 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

---

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 A37.
5 Norme ISA 200, paragraphes 15-16.
6 Norme ISA 200, paragraphe A46 et norme ISA 330, *Réponses de l'auditeur à l'évaluation des risques*, paragraphe 6.

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 ».

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 exigences et des modalités d'application supplémentaires sont fournies dans la norme ISA 240[7] 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 exigences 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 financiers[8]. 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 risques évalués d'anomalies significatives au niveau des assertions et y répondent[9].

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 exigences à toutes les entités, que leur nature et leurs circonstances soient peu complexes ou très complexes[10]. 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.

---

7 Norme ISA 240, *Responsabilités de l'auditeur concernant les fraudes lors d'un audit d'états financiers*.
8 Norme ISA 330, paragraphe 5.
9 Norme ISA 330, paragraphe 6.
10 Norme ISA 200, paragrapheA69.

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.

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 fraude[11], dans la mesure où ils influent sur le risque inhérent ; (Voir par. A7-A8)

[11] Norme ISA 240, paragraphes A24-A27.

(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 ;

(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 exigences d'autres normes ISA, être considéré comme un risque important[12] ;

(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,

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

(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.

    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

<table>
<tr><td colspan="2">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)</td></tr>
<tr><td>(a) comprendre l'ensemble des contrôles, des processus et de l'organisation prenant en compte : (Voir par. A101- A102)

(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</td><td>(b) évaluer : (Voir par. A103-A108)

(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,</td></tr>
</table>

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 ;	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 :	
(a) comprendre le processus suivi par l'entité pour : (Voir par. A109-A110) (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 ;	(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)

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

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)	
(a) comprendre les aspects du processus de l'entité traitant : (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)	et (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)

(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-A120)	

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

Le système d'information et de communication

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)	
(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 : 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 b. comment les informations sur des événements et des circonstances, autres que les opérations, sont saisies, traitées et fournies dans les états financiers, (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, (iii) le processus d'élaboration de l'information financière utilisé pour préparer les états financiers de l'entité, y compris les informations à fournir, (iv) les ressources de l'entité, y compris son environnement informatique, qui sont pertinentes au regard des paragraphes (a)(i)-(a)(iii) ci-dessus ; (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)	Et (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)

(i) les personnes au sein de l'entité, y compris la communication des rôles et des responsabilités en matière d'information financière, (ii) la direction et les personnes constituant le gouvernement d'entreprise, (iii) l'entité et les parties externes, par exemple les autorités de contrôle ;	

Mesures de contrôle

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)	
(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 : (i) les contrôles qui répondent à un risque qualifié comme étant un risque important, (Voir par. A158-A159) (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) (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 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) (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) (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) (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) (i) les risques s'y rapportant, provenant du recours à l'informatique; et	Et (d) pour chaque contrôle identifié au paragraphe (a) ou (c)(ii) : (Voir par. A175-A181) (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 (ii) déterminer si le contrôle a été mis en œuvre, en exécutant d'autres procédures complémentairement à ses demandes d'informations auprès du personnel de l'entité.

(ii) les contrôles généraux sur le système informatique visant à répondre à ces risques ;	

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 identifiée(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'audit[13] : (Voir par. A237-A241)

    (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 exigences 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.

*****

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

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 580[14], 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).

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

[14] Norme ISA 580, *Déclarations écrites*.

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 exigences 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 fraudes[15]. En outre, les normes ISA suivantes fournissent 'd'autres exigences 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:

- la norme ISA 540 (révisée)[16], pour les estimations comptables ;
- la norme ISA 550, pour les relations et les opérations avec les parties liées ;

[15] Norme ISA 240, paragraphes 12-27.
[16] Norme ISA 540 (révisée), *Audit des estimations comptables et des informations à fournir les concernant*.

- la norme ISA 570 (révisée)[17], pour la continuité de l'exploitation ;
- la norme ISA 600[18], 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'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 sources[19], 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.

[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 500[20].

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 exigences 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 500[21]. 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'audit[22]. 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

[20] Norme ISA 500, *Éléments probants*, paragraphe 7.
[21] Norme ISA 500, paragraphes A14-A17 et A21-A25.
[22] Norme ISA 500, paragraphe A12.

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 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 réexécutions 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.

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.

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

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 520[24] 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

[24] Norme ISA 520, *Procédures analytiques*.

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 exigences de la norme ISA 520. Cependant, les exigences 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.

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 ;

[25] Norme ISA 220 (révisée), *Gestion de la qualité d'un audit d'états financiers*, paragraphe 22-24.

- 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.

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 240[26] 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.

[26] Norme ISA 240, paragraphe 16.

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.

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 320[29] ;
- évalue le caractère approprié du choix et de l'application des méthodes comptables et le caractère adéquat des informations fournies dans les états financiers.

[27] Norme ISA 250 (révisée), *Prise en considération des textes législatifs et réglementaires dans un audit d'états financiers*, paragraphe 14.
[28] Norme ISA 700 (révisée), *Opinion et rapport sur des états financiers,* paragraphe 13(e).
[29] Norme ISA 320, *Caractère significatif dans la planification et la réalisation d'un audit*, paragraphes 10-11.

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 520[30] ;
- 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).

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 ;

[30] Norme ISA 520, paragraphe 5.

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 financiers[31] ;
- 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 minime, voire inexistante; dans d'autres entités, notamment celles qui sont cotées, cette distinction peut être très claire[32].

- 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

[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.

[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.

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 connaitre la capacité de l'entité à exercer une surveillance adéquate sur son système de contrôle interne. Elle peut aussi l'aider à relever des 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 ; ou
- 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 réglementations ou les instructions d'une autre autorité .

Facteurs relatifs au secteur d'activité, facteurs réglementaires et autres facteurs externes (Voir par. 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 la compétence et les capacités appropriées[33].

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 exigences portant spécifiquement sur le cadre légal et réglementaire applicable à l'entité et à son secteur d'activité[34].

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.

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 exigences et les indications relatives aux risques de fraude sont détaillées dans la norme ISA 240).

[33] Norme ISA 220 (révisée), paragraphe 25-28.
[34] Norme ISA 250 (révisée), paragraphe 13.

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

connaitre 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 reconnaitre, 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 exigences contenues dans les normes ISA (voir les paragraphes A95, A103, A111, A121, A124 et A151), peuvent aussi influer 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 reliés.

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 connaitre 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 influer 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 influer 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 complémentaires[35].

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

[35] Norme ISA 330, paragraphes A1-A3.

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

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 commises[36].

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.

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

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 par. A86).

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 par. 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 influer 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**, paragraphes 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 livrel 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 capacité[38].

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.

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.

[38] Norme ISA 570 (révisée), paragraphes 19-20.

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 influer 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 contrôles[39].

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 330[40], se baser sur la connaissance acquise relative à la manière dont la direction répond aux risques importants. Bien que les risques 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 :

[39] Norme ISA 240, paragraphe A28.
[40] Norme ISA 330, paragraphe 21.

- 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 240[41] 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.

[41] Norme ISA 240, paragraphes 28 et A33.

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 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 330[42] 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 330[43] 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 influer 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'en 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 ;

[42] Norme ISA 330, paragraphe 8(b).
[43] Norme ISA 330, paragraphe 8 a).

- les contrôles complémentaires de l'entité utilisatrice, si l'entité fait appel à une société de services[44].

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 influer 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 influer 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 ;

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

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 sujets 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 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 330[45].

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.

[45] Norme ISA 330, paragraphes 8-11.

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'entité[46], 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 265[47] 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 importante[48].

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

[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.

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 concrétisent[49].

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.

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,

[49] Norme ISA 200, paragraphe A16.

(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 330[50].

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 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.

[50] Norme ISA 330, paragraphe 5.

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 exigences 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.

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 .

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

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 identifiés[52] ;
- 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 élevé[53] ;
- 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 identifiés[54] ;
- 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'audit[55] ;
- 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 mission[56] ;
- 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 composant[57].

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 » différera 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 exigences

[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 32 et A87-A89.
[57] Norme ISA 600, paragraphes 30-31.

d'une autre norme ISA. La norme ISA 240 contient d'autres exigences et indications concernant l'identification et l'évaluation des risques d'anomalies significatives résultant de fraudes[58].

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 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

[58] Norme ISA 240, paragraphes 26-28.

probants suffisants et appropriés, étant donné que l'auditeur doit, conformément à la norme ISA 330[59], concevoir et mettre en œuvre des tests sur ces contrôles.

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 appropriés[60]. 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.

[59] Norme ISA 330, paragraphe 8.
[60] Norme ISA 540 (révisée), paragraphes A87-A89.

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 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 circonstances[61].

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 contredisent[62].

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

[61] Norme ISA 330, paragraphes A29-A30.
[62] Norme ISA 500, paragraphe A1.

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 320[63], 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 besoins d'information financière des utilisateurs des états financiers[64]. 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.

[63] Norme ISA 320, paragraphe A1.
[64] Norme ISA 320, paragraphe 4.
[65] Norme ISA 330, paragraphe 18.

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 critique[66]. 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 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 exigences 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 ;

[66] Norme ISA 230, paragraphe A7.

- 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 clés[67] 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.

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 travail[68]. 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 complémentaires[69].

[67] Norme ISA 230, paragraphe 8.
[68] Norme ISA 300, *Planification d'un audit d'états financiers*, paragraphes 7, 9 et A11.
[69] Norme ISA 330, paragraphe 28.

Annexe 1
(Voir par. A61-A67)

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'entité[70].

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 fraude[71], 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

[71] Norme ISA 240, paragraphes A24-A27.

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.

- *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 influer 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	Réglementation : • Activités soumises à une réglementation très complexe. Modèle économique : • Existence d'alliances complexes et de co-entreprises. Référentiel comptable applicable : • Évaluations comptables impliquant des processus complexes. Opérations : • Recours à des financements hors-bilan, entités ad hoc, et autres mécanismes complexes de financement.
Subjectivité	Référentiel comptable applicable : • 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	Conjoncture économique : • Activités menées dans des régions qui sont économiquement instables, par exemple, des pays avec des dévaluations monétaires importantes ou une économie fortement inflationniste. Marchés : • Activités exposées à des marchés volatils par exemple, le marché des contrats à terme). Perte de clients : • Problème de continuité d'exploitation ou de liquidités, y compris la perte de clients importants. Modèle sectoriel : • Changements dans le secteur d'activité dans lequel l'entité opère. Modèle économique : • Modifications dans la chaîne d'approvisionnements.

Facteur de risque inhérent	Exemples d'événements ou de situations pouvant indiquer l'existence de risques d'anomalies significatives au niveau des assertions
	• Développement ou offre de nouveaux produits ou services, ou diversification dans de nouvelles activités. Situation géographique : • Expansion vers de nouvelles localisations. Structure de l'entité : • 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. Ressources humaines : • Changements dans le personnel-clé, y compris le départ de dirigeants-clés. Informatique : • Changements dans l'environnement informatique. • Installation de nouveaux systèmes informatiques importants liés à l'élaboration de l'information financière. Référentiel comptable applicable : • Application de nouvelles normes comptables. Capital : • Nouvelles Restrictions sur la disponibilité du capital et du crédit Réglementation : • 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	Informations : • 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	Informations : • 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). Transactions : • 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'entité[72]. Le processus de suivi de ce système par l'entité peut inclure des

[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.

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).

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 autorisé* — 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.

25.

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'efficience et de l'efficacité 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[73]. 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.

[73] Les exigences pertinentes sont contenues dans la norme ISA 610 (révisée en 2013).

4. Si sur la base des réponses aux questions de l'auditeur, il apparait 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[74], 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.

[74] Norme ISA 240, paragraphe 19.

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[75], 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.

[75] Norme ISA 200, paragraphe 7.

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			
• 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
• 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
• 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
• 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
• 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[76] ; 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			
• Type d'applications (par exemple, applications commerciales peu ou pas	Applications commerciales peu ou pas personnalisées	Applications commerciales, applications	Applications développées sur mesure ou

[76] 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.

personnalisées ou, au contraire, applications très personnalisées ou fortement intégrées, qui ont été soit achetées et personnalisées soit développées en interne)		développées en interne peu complexes, ou progiciel de gestion intégré d'entrée de gamme peu ou pas personnalisé	progiciels de gestion intégrés complexes et hautement personnalisés
• 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 dans le Cloud (« SAAS Cloud »)	Ordinateur central complexe ; client-serveur important ou complexe ; applications Web ; (infrastructure hébergée dans le Cloud)
• 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
• 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			
• 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
• Complexité des processus de gestion des droits d'accès	Droits d'accès gérés par une seule personne détenant	Droits d'accès gérés par un petit nombre de personnes	Droits d'accès gérés par le service informatique au

	des droits d'administrateur	détenant des droits d'administrateur	moyen de processus complexes
• 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 effectuées au moyen du Web ou d'interfaces externes	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
• 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
• 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
• Conversion de données majeure au cours de la période et, le cas échéant, nature et importance des changements apportés et	Mises à niveau logicielles provenant du fournisseur, sans conversion des données	Mises à niveau mineures pour les applications logicielles commerciales nécessitant peu de	Mise à niveau majeure, nouvelle version, changement de plateforme

méthode de conversion utilisée		conversion de données	

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'efficience 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 influer 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

• Applications autonomes
• Volume de données (opérations) peu important
• Fonctionnalités peu complexes
• Opérations systématiquement étayées par les originaux papier
	• Applications avec interfaces
	• Volume de données (opérations) important
	• Fonctionnalités complexes, telles que :
	  ○ 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 : • 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.	Raisons pour lesquelles ces applications informatiques sont généralement sujettes aux risques provenant du recours à l'informatique : • 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), 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.

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. 26(c) 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**		
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 accès	Privilèges d'accès : Utilisateurs détenant des privilèges d'accès	La nature et l'étendue des privilèges	Oui, au lieu de l'examen des accès	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) ?**
	supérieurs à ceux qui sont nécessaires pour l'exercice de leurs fonctions, ce qui peut compromettre la séparation des tâches.	d'accès modifiés ou nouvellement attribués sont approuvées par la direction, notamment en ce qui concerne les rôles/profils standardisés d'utilisateurs des applications, les opérations donnant lieu à des informations financières critiques et la séparation des tâches.	utilisateurs mentionné ci-après		
		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

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) ?**
		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 exemple, les droits d'administrateurs permettant de gérer la configuration, les données et la sécurité) sont strictement attribués aux utilisateurs autorisés.	Oui, mais probablement seulement au niveau de la couche « applications informatiques »	Oui, au niveau de la couche « applications informatiques » et de certaines couches « environnement informatique » de la plateforme	Oui, à toutes les couches « 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	L'accès aux fichiers de données des applications ou aux objets, tables ou données des	N/A	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) ?**
	soit enregistrée dans une application.	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.			
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 appropriés et dûment autorisés.	Pour accéder aux systèmes, les utilisateurs doivent s'authentifier au moyen de codes d'utilisateur et de mots de passe uniques ou d'autres mécanismes de validation des droits d'accès. Les paramètres des mots de passe répondent aux normes de l'entreprise ou du secteur (longueur minimale et niveau de complexité exigés,	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) ?**
		expiration du mot de passe, verrouillage du compte, etc.).			
		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
Gestion des changements	Applications : Modification inappropriée des systèmes/programmes d'application dotés de contrôles automatisés pertinents (paramètres configurables, algorithmes/calculs automatisés, extraction automatisée des données, etc.) ou de fonctionnalités logiques permettant de générer des rapports.	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
		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	N/A	Oui, s'il s'agit de logiciels non commerciaux	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) ?**
		de développement.			
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	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) ?**
		d'autres mécanismes de validation des droits d'accès. 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.).			
		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.	N/A, réseau non segmenté	Oui, en faisant preuve de jugement	Oui, en faisant preuve de jugement
		Les gestionnaires du réseau	N/A	Oui, en faisant preuve de jugement	Oui, en faisant preuve de jugement

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) ?**
		effectuent périodiquement des analyses de vulnérabilité du périmètre du réseau et procèdent à des investigations 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	N/A, pas de « VPN »	Oui, en faisant preuve de jugement	Oui, en faisant preuve de jugement

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) ?**
		autorisés et appropriés.			
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
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	N/A, aucun suivi des travaux	Oui, pour certaines applications	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) ?**
		l'intégrité du traitement.			