Internationale controlestandaard 315 (herzien 2019)

ISA 315 (herzien 2019)

Risico's op een afwijking van materieel belang identificeren en inschatten

IAASB International Auditing and Assurance Standards Board

Over de IAASB

Dit document werd ontwikkeld en goedgekeurd door de International Auditing and Assurance Standards Board (IAASB).
Deze IAASB ontwikkelt controle- en assurance-standaarden en leidraden voor gebruik door alle auditors onder een gedeeld proces voor het vaststellen van standaarden waarbij de Public Interest Oversight Board en de IAASB Consultative Advisory Group betrokken zijn. De Public Interest Oversight Board houdt toezicht op de activiteiten van de IAASB. De IAASB Consultative Advisory Group geeft inbreng op de ontwikkeling van standaarden en leidraden vanuit het openbaar belang.
De doelstelling van de IAASB is om het openbaar belang te dienen door het vaststellen van controle- en overige standaarden van hoge kwaliteit en door het faciliteren van de convergentie van internationale en nationale controle- en assurance-standaarden. Daarmee verhoogt zij de kwaliteit en consistentie van de praktijk in de hele wereld en versterkt zij het publieke vertrouwen in het wereldwijde accountantsberoep.

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

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I* - ISBN number: 978-1-60815-573-6.

INTERNATIONALE CONTROLESTANDAARD 315 (HERZIEN 2019)

RISICO'S OP EEN AFWIJKING VAN MATERIEEL BELANG IDENTIFICEREN EN INSCHATTEN

(van toepassing voor controles van financiële overzichten over verslagperioden die op of na 15 december 2021 van start gaan)(*)

(*) ISA 315 (Herzien 2019) bevat overeenstemmingswijzigingen die voortvloeien uit ISA 600 (Herzien). De inwerkingtreding van deze wijzigingen valt samen met deze ISA.

INHOUDSOPGAVE

Internationale Controlestandaard (ISA) 315 (herzien 2019), *Risico's op een afwijking van materieel belang identificeren en inschatten* dient te worden gelezen in samenhang met ISA 200, *Algehele doelstellingen van de onafhankelijke auditor, alsmede het uitvoeren van een controle overeenkomstig de Internationale Controlestandaarden*.
ISA 315 (herzien 2019) heeft de goedkeuring gekregen van de *Public Interest Oversight Board* (PIOB) die tot de conclusie is gekomen dat het *due process* werd gevolgd in de totstandkoming van de standaard en dat juiste aandacht werd besteed aan het openbaar belang.

Inleiding

Toepassingsgebied van deze ISA

1. Deze ISA behandelt de verantwoordelijkheid van de auditor om de risico's op een afwijking van materieel belang in de financiële overzichten te identificeren en in te schatten.

Belangrijke uitgangspunten in deze ISA

2. ISA 200 behandelt de algehele doelstellingen van de auditor bij het uitvoeren van een controle van de financiële overzichten[1], inclusief het verkrijgen van voldoende en geschikte controle-informatie om het controlerisico terug te brengen tot een aanvaardbaar laag niveau.[2] Controlerisico is een functie van de risico's op een afwijking van materieel belang en ontdekkingsrisico.[3] ISA 200 legt uit dat de risico's op een afwijking van materieel belang op twee niveaus kunnen bestaan:[4] op het niveau van de financiële overzichten als geheel; en op het niveau van beweringen voor transactiestromen, rekeningsaldi en toelichtingen.

3. ISA 200 vereist dat de auditor professionele oordeelsvorming toepast bij het plannen en uitvoeren van een controle en dat hij een controle plant en uitvoert met een professioneel-kritische instelling waarbij hij er rekening mee houdt dat er omstandigheden kunnen bestaan die ertoe leiden dat de financiële overzichten een afwijking van materieel belang bevatten.[5]

4. Risico's op het niveau van de financiële overzichten hebben een diepgaande invloed op de financiële overzichten als geheel en kunnen een groot aantal beweringen beïnvloeden. Risico's op een afwijking van materieel belang op het niveau van beweringen bestaan uit twee componenten, inherent en interne beheersingsrisico:

   - inherent risico wordt beschreven als de vatbaarheid van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting voor een afwijking die afzonderlijk of gezamenlijk met andere afwijkingen van materieel belang is, voordat er rekening wordt gehouden met de eventuele daarop betrekking hebbende interne beheersingsmaatregelen.
   - interne beheersingsrisico wordt beschreven als het risico dat een afwijking in een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting en die afzonderlijk of gezamenlijk met andere afwijkingen van materieel belang is, niet wordt voorkomen of niet tijdig door het interne beheersingssysteem van de entiteit wordt gedetecteerd en hersteld.

5. ISA 200 legt uit dat risico's op een afwijking van materieel belang worden ingeschat op het niveau van beweringen om de aard, timing en omvang van verdere controlewerkzaamheden te bepalen die nodig zijn om voldoende en geschikte controle-informatie te verkrijgen.[6] Voor de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen, vereist deze ISA een afzonderlijke inschatting van het inherente risico en het interne beheersingsrisico. Zoals uitgelegd in ISA 200, is het inherente risico hoger voor sommige beweringen en daarmee verband houdende transactiestromen, rekeningsaldi en toelichtingen dan voor andere. De mate waarin het inherente risico varieert, wordt in deze ISA aangeduid als het 'spectrum van inherent risico'.

6. Risico's op een afwijking van materieel belang die door de auditor zijn geïdentificeerd en ingeschat, omvatten zowel afwijkingen die het gevolg van zijn fouten of van fraude. Hoewel beide door deze ISA worden behandeld, is de significantie van fraude zodanig dat verdere vereisten en

---

1 ISA 200, *Algehele doelstellingen van de onafhankelijke auditor, alsmede het uitvoeren van een controle overeenkomstige de ISA's.*
2 ISA 200, paragraaf 17.
3 ISA 200, paragraaf 13(c).
4 ISA 200, paragraaf A37.
5 ISA 200, paragrafen 15-16.
6 ISA 200, paragraaf A46 en ISA 330, *Inspelen door de auditor op ingeschatte risico's*, paragraaf 6.

leidraden zijn opgenomen in ISA 240[7] met betrekking tot risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden voor het verkrijgen van informatie die wordt gebruikt om de risico's op een afwijking van materieel belang die het gevolg is van fraude te identificeren, in te schatten en daarop in te spelen.

7. Het risico-identificatie- en inschattingsproces van de auditor is iteratief en dynamisch. Het inzicht van de auditor in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit hangen onderling samen met concepten in de vereisten om de risico's op een afwijking van materieel belang te identificeren en in te schatten. Bij het verwerven van het inzicht vereist door deze ISA, kunnen initiële verwachtingen van risico's worden ontwikkeld, die verder kunnen worden verfijnd naarmate de auditor vordert met het risico-identificatie- en inschattingsproces. Bovendien vereisen deze ISA en ISA 330 van de auditor om de risico-inschattingen te herzien en verdere algemene manieren om in te spelen op de risico's en verdere controlewerkzaamheden te wijzigen, op basis van controle-informatie verkregen bij het uitvoeren van verdere controlewerkzaamheden in overeenstemming met ISA 330, of als nieuwe informatie wordt verkregen.

8. ISA 330 vereist dat de auditor algehele manieren dient op te zetten en te implementeren om op de ingeschatte risico's op een afwijking van materieel belang op het niveau van de financiële overzichten in te spelen.[8] ISA 330 legt verder uit dat de inschatting van de risico's door de auditor op een afwijking van materieel belang op het niveau van de financiële overzichten en de algehele manieren van inspelen door de auditor worden beïnvloed door het inzicht van de auditor in de interne beheersingsomgeving. ISA 330 vereist ook dat de auditor verdere controlewerkzaamheden opzet en uitvoert waarvan de aard, timing en omvang zijn gebaseerd op en die inspelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van beweringen.[9]

Schaalbaarheid

9. ISA 200 stelt dat sommige ISA's schaalbaarheidsoverwegingen bevatten die de toepassing van de vereisten voor alle entiteiten illustreren, ongeacht of hun aard en omstandigheden minder of meer complex zijn.[10] Deze ISA is bedoeld voor controles van alle entiteiten, ongeacht de omvang of complexiteit en de toepassingsgerichte teksten bevatten daarom specifieke overwegingen voor zowel minder als meer complexe entiteiten, in voorkomend geval. Hoewel de omvang van een entiteit een indicatie kan zijn van de complexiteit ervan, kunnen sommige kleinere entiteiten complex zijn en sommige grotere entiteiten minder complex zijn.

Ingangsdatum

10. Deze ISA is van toepassing voor controles van financiële overzichten voor verslagperioden beginnend op of na 15 december 2021.

Doelstelling

11. De doelstelling van de auditor is het identificeren en inschatten van de risico's op een afwijking van materieel belang als gevolg van fraude of fouten, op het niveau van de financiële overzichten en op het niveau van beweringen, zodat een basis wordt verkregen voor het opzetten en het implementeren van manieren om in te spelen op de ingeschatte risico's op een afwijking van materieel belang.

Definities

7 ISA 240, *De verantwoordelijkheden van de auditor met betrekking tot fraude in het kader van een controle van financiële overzichten.*
8 ISA 330, paragraaf 5.
9 ISA 330, paragraaf 6.
10 ISA 200, paragraaf A69.

12. Voor de toepassing van de ISA's hebben de volgende termen de hierna weergegeven betekenis:

(a) beweringen — al dan niet expliciete uitspraken met betrekking tot de opname, waardering, presentatie en toelichting van informatie in de financiële overzichten die inherent zijn aan de bevestiging door het management dat de financiële overzichten in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving zijn opgesteld. Beweringen worden door de auditor gebruikt om de verschillende soorten mogelijke afwijkingen die kunnen voorkomen te overwegen bij het identificeren, inschatten van en inspelen op de risico's op een afwijking van materieel belang. (Zie par. A1)

(b) bedrijfsrisico – een risico dat voortkomt uit significante voorwaarden, gebeurtenissen, omstandigheden, handelingen of het achterwege laten van handelingen die een nadelig effect kunnen hebben op de mogelijkheid van een entiteit om haar doelstellingen te bereiken en haar strategieën uit te voeren, of dat voortkomt uit het vaststellen van ongepaste doelstellingen en strategieën.

(c) interne beheersingsmaatregelen – beleidslijnen of procedures die een entiteit vaststelt om de beheersingsdoelstellingen van management of de met governance belaste personen te bereiken. In deze context: (Zie par. A2-A5)

  (i) beleidslijnen zijn bepalingen over wat wel of niet binnen de entiteit dient te worden gedaan om de interne beheersing te bewerkstelligen. Dergelijke uiteenzettingen kunnen zijn gedocumenteerd, expliciet vermeld in mededelingen, of impliciet door handelingen en beslissingen.
  (ii) procedures zijn handelingen om beleidslijnen te implementeren.

(d) *general IT controls* – interne beheersingsmaatregelen over de informatietechnologie (IT)-processen van de entiteit die de voortdurende goede werking van de IT-omgeving ondersteunen, inclusief de voortdurende effectieve werking van interne beheersingsmaatregelen voor informatieverwerking en de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldigheid van informatie) in het informatiesysteem van de entiteit. Zie ook de definitie van IT-omgeving.

(e) interne beheersingsmaatregelen voor informatieverwerking – interne beheersingsmaatregelen in verband met de verwerking van informatie in IT applicaties of handmatige informatieprocessen in het informatiesysteem van de entiteit die rechtstreeks inspelen op risico's voor de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldigheid van transacties en andere informatie). (Zie par. A6)

(f) inherente risicofactoren – kenmerken van gebeurtenissen of omstandigheden die de vatbaarheid voor afwijkingen beïnvloeden, die het gevolg zijn van fraude of fouten, van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting, voordat rekening wordt gehouden met interne beheersingsmaatregelen. Dergelijke factoren kunnen kwalitatief of kwantitatief zijn en omvatten complexiteit, subjectiviteit, wijzigingen, onzekerheid of vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of andere frauderisicofactoren[11] voor zover ze het inherente risico beïnvloeden. (Zie par. A7-A8)

(g) IT-omgeving – de IT-applicaties en ondersteunende IT-infrastructuur, evenals de IT-processen en personeel betrokken bij die processen, die een entiteit gebruikt om bedrijfsactiviteiten te ondersteunen en bedrijfsstrategieën te bereiken. Voor de toepassing van deze ISA geldt het volgende:

  (i) een IT-applicatie is een programma of een reeks programma's die worden gebruikt bij het initiëren, verwerken, vastleggen en rapporteren van transacties of informatie. IT-applicaties omvatten ook datawarehouses en rapportgenerators.
  (ii) de IT-infrastructuur omvat het netwerk, besturingssystemen en databases en hun gerelateerde hardware en software.
  (iii) de IT-processen zijn de processen van de entiteit om de toegang tot de IT-omgeving te beheren, programmawijzigingen of wijzigingen in de IT-omgeving te beheren en IT-activiteiten te beheren.

[11] ISA 240, paragrafen A24-A27.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

(h) relevante beweringen – een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting is relevant wanneer voor die bewering een geïdentificeerd risico op een afwijking van materieel belang bestaat. De bepaling of een bewering een relevante bewering is, wordt gemaakt voordat rekening wordt gehouden met de eventuele daarop betrekking hebbende interne beheersingsmaatregelen (d.w.z., het inherente risico). (Zie par. A9)

(i) risico's die voortkomen uit het gebruik van IT – vatbaarheid van interne beheersingsmaatregelen voor informatieverwerking voor ineffectieve opzet of werking, of risico's voor de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldigheid van transacties en andere informatie) in het informatiesysteem van de entiteit als gevolg van ineffectieve opzet of werking van interne beheersingsmaatregelen in de IT-processen van de entiteit (zie IT-omgeving).

(j) risico-inschattingswerkzaamheden – de controlewerkzaamheden die zijn opgezet en uitgevoerd om de risico's op een afwijking van materieel belang als gevolg van fraude of fouten te identificeren en in te schatten op het niveau van de financiële overzichten en op het niveau van beweringen.

(k) significante transactiestroom, rekeningsaldo of toelichting – een transactiestroom, rekeningsaldo of toelichting waarvoor er een of meer relevante beweringen zijn.

(l) Significant risico - Een geïdentificeerd risico op een afwijking van materieel belang: (Zie par. A10)

  (i) waarvoor de inschatting van het inherente risico dicht bij de bovengrens van het spectrum van inherent risico is vanwege de mate waarin inherente risicofactoren de combinatie van de waarschijnlijkheid dat een afwijking voorkomt en de orde van grootte van de potentiële afwijking indien die afwijking zich zou voordoen, beïnvloeden; of
  (ii) dat moet worden behandeld als een significant risico in overeenstemming met de vereisten van andere ISA's.[12]

(m) systeem van interne beheersing – het systeem dat is ontworpen, geïmplementeerd en onderhouden door de met governance belaste personen, management en ander personeel om een redelijke mate van zekerheid te verschaffen over het bereiken van de doelstellingen van een entiteit met betrekking tot de betrouwbaarheid van financiële verslaggeving, effectiviteit en efficiëntie van activiteiten en naleving van de van toepassing zijnde wet- en regelgeving. Voor de toepassing van de ISA's bestaat het interne beheersingssysteem uit vijf onderling verbonden componenten:

  (i) interne beheersingsomgeving;
  (ii) het risico-inschattingsproces van de entiteit;
  (iii) het proces van de entiteit om het interne beheersingssysteem te monitoren;
  (iv) het informatiesysteem en communicatie; en
  (v) interne beheersingsactiviteiten.

Vereisten

Risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden

13. De auditor dient risico-inschattingswerkzaamheden op te zetten en uit te voeren om controle-informatie te verkrijgen die een geschikte basis biedt voor: (Zie par. A11-A18)

  (a) de identificatie en inschatting van risico's op een afwijking van materieel belang als gevolg van fraude of fouten, op het niveau van de financiële overzichten en beweringen; en
  (b) de opzet van verdere controlewerkzaamheden in overeenstemming met ISA 330.

[12] ISA 240, paragraaf 27 en ISA 550, *Verbonden partijen*, paragraaf 18.

De auditor dient risico-inschattingswerkzaamheden op te zetten en uit te voeren op een manier die niet tendeert naar het verkrijgen van controle-informatie die bevestigend kan zijn of naar het uitsluiten van controle-informatie die tegenstrijdig kan zijn. (Zie par. A14)

14. De risico-inschattingswerkzaamheden omvatten het volgende: (Zie par. A19-A21)

    (a) verzoeken om inlichtingen bij het management en bij andere geschikte personen binnen de entiteit, inclusief personen binnen de interne auditfunctie (als de functie bestaat). (Zie par. A22-A26)
    (b) cijferanalyses. (Zie par. A27-A31)
    (c) waarneming en inspectie. (Zie par. A32-A36)

Informatie uit andere bronnen

15. Bij het verkrijgen van controle-informatie in overeenstemming met paragraaf 13 dient de auditor informatie in overweging te nemen van: (Zie par. A37-A38)

    (a) de werkzaamheden van de auditor met betrekking tot aanvaarding of continuering van de cliëntrelatie of de controle-opdracht; en
    (b) indien van toepassing, andere opdrachten die door de opdrachtpartner voor de entiteit zijn uitgevoerd.

16. Wanneer de auditor voornemens is informatie te gebruiken die is verkregen uit eerdere ervaringen van de auditor met de entiteit en uit controlewerkzaamheden die zijn uitgevoerd in eerdere controles, dient de auditor te evalueren of dergelijke informatie relevant en betrouwbaar blijft als controle-informatie voor de lopende controle. (Zie par. A39-A41)

Bespreking opdrachtteam

17. De opdrachtpartner en andere kernleden van het opdrachtteam bespreken de toepassing van het van toepassing zijnde stelsel inzake financiële verslaggeving en de vatbaarheid van de financiële overzichten van de entiteit voor een afwijking van materieel belang. (Zie par. A42-A47)

18. Wanneer er leden van het opdrachtteam niet betrokken zijn bij de bespreking van het opdrachtteam, dient de opdrachtpartner te bepalen welke aangelegenheden aan die leden moeten worden meegedeeld.

Het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit (Zie par. A48-A49)

Inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving (Zie par. A50-A55)

19. De auditor dient risico-inschattingswerkzaamheden uit te voeren om inzicht te verwerven in:

    (a) de volgende aspecten van de entiteit en haar omgeving:

        (i) de organisatiestructuur, eigendom en governance van de entiteit en haar bedrijfsmodel, inclusief de mate waarin het bedrijfsmodel het gebruik van IT integreert; (Zie par. A56-A67)
        (ii) sector, regelgevende en andere externe factoren; (Zie par. A68-A73) en
        (iii) de maatregelen die intern en extern zijn gebruikt om de financiële prestaties van de entiteit te beoordelen; (Zie par. A74-A81)

(b) het van toepassing zijnde stelsel inzake financiële verslaggeving en de grondslagen voor financiële verslaggeving van de entiteit en de redenen voor eventuele wijzigingen daarin; (Zie par. A82-A84) en
(c) hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden en de mate waarin zij dit doen bij het opstellen van de financiële overzichten in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving, op basis van de onder (a) en (b) verworven inzichten. (Zie par. A85-A89)

20. De auditor dient te evalueren of de grondslagen voor financiële verslaggeving van de entiteit passend en consistent zijn met het van toepassing zijnde stelsel inzake financiële verslaggeving.

Inzicht in de componenten van het interne beheersingssysteem van de entiteit (Zie par. A90-A95)

Interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het interne beheersingssysteem te monitoren (Zie par. A96-A98)

Interne beheersingsomgeving

21. De auditor dient door het uitvoeren van risico-inschattingswerkzaamheden inzicht te verwerven in de interne beheersingsomgeving die relevant is voor het opstellen van de financiële overzichten, door: (Zie par. A99-A100)	
(a) inzicht te verwerven in de interne beheersingsmaatregelen, processen en structuren die betrekking hebben op: (Zie par. A101-A102) (i) hoe de verantwoordelijkheden van het management om toezicht uit te oefenen worden uitgevoerd, zoals de cultuur van de entiteit en de toewijding van het management aan integriteit en ethische waarden; (ii) wanneer de met governance belaste personen gescheiden zijn van het management, de onafhankelijkheid van en toezicht op het interne beheersingssysteem van de entiteit door de met governance belaste personen; (iii) de toewijzing door de entiteit van bevoegdheden en verantwoordelijkheid; (iv) hoe de entiteit competente personen aantrekt, ontwikkelt en behoudt; en (v) hoe de entiteit personen verantwoording laat afleggen over hun verantwoordelijkheden bij het nastreven van de doelstellingen van het interne beheersingssysteem;	en (b) te evalueren of: (Zie par. A103-A108) (i) management, met het toezicht van de met governance belaste personen, een cultuur van eerlijkheid en ethisch gedrag heeft gecreëerd en gehandhaafd; (ii) de interne beheersingsomgeving een geschikte basis verschaft voor de andere componenten van het interne beheersingssysteem van de entiteit gezien de aard en complexiteit van de entiteit; en (iii) tekortkomingen in de interne beheersing geïdentificeerd in de interne beheersingsomgeving de andere componenten van het interne beheersingssysteem van de entiteit ondermijnen.

Het risico-inschattingsproces van de entiteit

22. De auditor dient door het uitvoeren van risico-inschattingswerkzaamheden inzicht te verwerven in het risico-inschattingsproces van de entiteit dat relevant is voor het opstellen van de financiële overzichten, door:	
(a) inzicht te verwerven in het proces van de entiteit voor: (Zie par. A109-A110)	en (b) te evalueren of het risico-inschattingsproces van de entiteit geschikt is voor de

(i) het identificeren van bedrijfsrisico's die relevant zijn voor de doelstellingen van de financiële verslaggeving; (Zie par. A62) (ii) het inschatten van de significantie van die risico's, inclusief de waarschijnlijkheid dat deze voorkomen; en (iii) het inspelen op die risico's;	omstandigheden van de entiteit gezien de aard en complexiteit van de entiteit. (Zie par. A111-A113)

23. Als de auditor risico's op een afwijking van materieel belang identificeert die het management niet heeft geïdentificeerd, dient hij:

(a) te bepalen of dergelijke risico's van een soort zijn waarvan de auditor verwacht dat deze geïdentificeerd worden door het risico-inschattingsproces van de entiteit en, zo ja, inzicht te verwerven in de reden dat het risico-inschattingsproces van de entiteit dergelijke risico's op een afwijking van materieel belang niet heeft geïdentificeerd; en
(b) de implicaties voor de evaluatie van de auditor in paragraaf 22(b) te overwegen.

Het proces van de entiteit om het interne beheersingssysteem te monitoren

24. De auditor dient door het uitvoeren van risico-inschattingswerkzaamheden inzicht te verwerven in het proces van de entiteit voor het monitoren van het interne beheersingssysteem dat relevant is voor het opstellen van de financiële overzichten, door: (Zie par. A114-A115)	
(a) inzicht te verwerven in die aspecten van het proces van de entiteit die betrekking hebben op: (i) voortdurende en afzonderlijke evaluaties voor het monitoren van de effectiviteit van interne beheersingsmaatregelen en de identificatie en het herstel van geïdentificeerde tekortkomingen in de interne beheersing; (Zie par. A116-A117) en (ii) de interne auditfunctie van de entiteit, indien aanwezig, inclusief haar aard, verantwoordelijkheden en activiteiten; (Zie par. A118) (b) inzicht te verwerven in de bronnen van de informatie die gebruikt wordt in het proces van de entiteit om het interne beheersingssysteem te monitoren en de basis waarop management de informatie als voldoende betrouwbaar voor het doel overweegt; (Zie par. A119-A120)	en (c) te evalueren of het proces voor het monitoren van het interne beheersingssysteem van de entiteit geschikt is voor de omstandigheden van de entiteit gezien de aard en complexiteit van de entiteit. (Zie par. A121-A122)

Informatiesysteem en communicatie, en interne beheersingsactiviteiten (Zie par. A123-A130)

Het informatiesysteem en communicatie

25. De auditor dient door middel van risico-inschattingswerkzaamheden inzicht te verwerven in het informatiesysteem en de communicatie van de entiteit die relevant is voor het opstellen van de financiële overzichten, door: (Zie par. A131)	
(a) inzicht te verwerven in de informatieverwerkingsactiviteiten van de	en

entiteit, inclusief gegevens en informatie, de benodigde middelen voor dergelijke activiteiten en de beleidslijnen die voor significante transactiestromen, rekeningsaldi en toelichtingen definiëren: (Zie par. A132-A143) (i) hoe informatie stroomt door het informatiesysteem van de entiteit, inclusief hoe: a. transacties worden geïnitieerd, en hoe informatie daarover wordt vastgelegd, verwerkt, gecorrigeerd indien nodig, opgenomen in het grootboek en gerapporteerd in de financiële overzichten; en b. informatie over gebeurtenissen en omstandigheden, anders dan transacties, wordt vastgelegd, verwerkt en toegelicht in de financiële overzichten; (ii) de administratieve vastleggingen, specifieke rekeningen in de financiële overzichten en andere ondersteunende vastleggingen met betrekking tot de informatiestromen in het informatiesysteem; (iii) het proces van financiële verslaggeving dat is gebruikt om de financiële overzichten van de entiteit, inclusief toelichtingen, op te stellen; en (iv) de middelen van de entiteit, inclusief de IT-omgeving, relevant voor (a) (i) tot (a) (iii) hierboven; (b) inzicht te verwerven in hoe de entiteit significante aangelegenheden communiceert die het opstellen van de financiële overzichten en gerelateerde rapporteringsverantwoordelijkheden in het informatiesysteem en andere componenten van het interne beheersingssysteem ondersteunen: (Zie par. A144-A145) (i) tussen mensen binnen de entiteit, inclusief hoe financiële verslaggevingstaken en verantwoordelijkheden worden gecommuniceerd; (ii) tussen management en de met governance belaste personen; en (iii) met externe partijen, zoals die met regelgevende of toezichthoudende instanties;	(c) te evalueren of het informatiesysteem van de entiteit en de communicatie op gepaste wijze het opstellen van de financiële overzichten van de entiteit in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving ondersteunen. (Zie par. A146)

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

Interne beheersingsactiviteiten

26. De auditor dient inzicht te verwerven in de component "interne beheersingsactiviteiten" door middel van uitvoering van risico-inschattingswerkzaamheden, door: (Zie par. A147-A157)

(a) het identificeren van interne beheersingsmaatregelen die inspelen op risico's op een afwijking van materieel belang op het niveau van beweringen in de component "interne beheersingsactiviteiten" als volgt:

  (i) interne beheersingsmaatregelen die inspelen op een risico dat is bepaald als een significant risico; (Zie par. A158-A159)
  (ii) interne beheersingsmaatregelen over journaalboekingen, inclusief niet-standaard journaalboekingen die worden gebruikt om niet-terugkerende, ongebruikelijke transacties of aanpassingen vast te leggen; (Zie par. A160-A161)
  (iii) interne beheersingsmaatregelen waarvoor de auditor van plan is de effectieve werking te toetsen bij het bepalen van de aard, timing en omvang van gegevensgerichte werkzaamheden, waaronder interne beheersingsmaatregelen die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen geen voldoende en geschikte controle-informatie bieden; en (Zie par. A162-A164)
  (iv) andere interne beheersingsmaatregelen waarvan de auditor overweegt dat deze geschikt zijn om de auditor in staat te stellen de doelstellingen van paragraaf 13 te bereiken met betrekking tot risico's op het niveau van beweringen, op basis van de professionele oordeelsvorming van de auditor; (Zie par. A165)

(b) gebaseerd op de onder (a) geïdentificeerde interne beheersingsmaatregelen, het identificeren van de IT-applicaties en de andere aspecten van de IT omgeving van de entiteit die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT; (Zie par. A166-A172)

(c) voor dergelijke IT-applicaties en andere aspecten van de IT omgeving geïdentificeerd in (b), het identificeren van: (Zie par. A173-A174)

  (i) de bijbehorende risico's die voortkomen uit het gebruik van IT; en

en

(d) voor elke interne beheersingsmaatregel onder (a) of (c) (ii): (Zie par. A175-A181)

  (i) te evalueren of de interne beheersingsmaatregel effectief is opgezet om in te spelen op het risico op een afwijking van materieel belang op het niveau van beweringen, of effectief is opgezet om de werking van andere interne beheersingsmaatregelen te ondersteunen; en
  (ii) te bepalen of de interne beheersingsmaatregel is geïmplementeerd door het uitvoeren van werkzaamheden in aanvulling op verzoeken om inlichtingen bij het personeel van de entiteit.

(ii) De *general IT-controls* van de entiteit die inspelen op dergelijke risico's;	

Tekortkomingen binnen het interne beheersingssysteem van de entiteit

27. Gebaseerd op de evaluatie door de auditor van elk van de componenten van het interne beheersingssysteem van de entiteit, dient de auditor te bepalen of een of meer tekortkomingen in de interne beheersing zijn geïdentificeerd. (Zie par. A182-A183)

Het identificeren en inschatten van de risico's op een afwijking van materieel belang (Zie par. A184-A185)

Identificeren van risico's op een afwijking van materieel belang

28. De auditor dient de risico's op een afwijking van materieel belang te identificeren en te bepalen of deze bestaan op: (Zie par. A186-A192)

    (a) het niveau van de financiële overzichten; (Zie par. A193-A200) of
    (b) het niveau van beweringen voor transactiestromen, rekeningsaldi en toelichtingen. (Zie par. A201)

29. De auditor dient de relevante beweringen en de bijbehorende significante transactiestromen, rekeningsaldi en toelichtingen te bepalen. (Zie par. A202-A204)

Het inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten

30. Voor geïdentificeerde risico's op een afwijking van materieel belang op het niveau van de financiële overzichten, dient de auditor de risico's in te schatten en: (Zie par. A193-A200)

    (a) te bepalen of dergelijke risico's de inschatting van risico's op het niveau van beweringen beïnvloeden; en
    (b) de aard en omvang van hun diepgaande invloed op de financiële overzichten te evalueren.

Inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen

Inschatting van het inherente risico (Zie par. A205-A217)

31. Voor geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen, dient de auditor het inherente risico in te schatten door de waarschijnlijkheid en de orde van grootte van een afwijking in te schatten. Daarbij dient de auditor rekening te houden met hoe en in welke mate:

    (a) inherente risicofactoren de vatbaarheid van relevante beweringen voor afwijkingen beïnvloeden; en
    (b) de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten de inschatting van inherent risico voor risico's op een afwijking van materieel belang op het niveau van beweringen beïnvloeden. (Zie par. A215-A216)

32. De auditor dient te bepalen of een of meer van de ingeschatte risico's op een afwijking van materieel belang een significant risico is. (Zie par. A218-A221)

33. De auditor dient te bepalen of gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie kunnen verschaffen voor de risico's op een afwijking van materieel belang op het niveau van beweringen. (Zie par. A222-A225)

Inschatting van het interne beheersingsrisico

34. Als de auditor van plan is de effectieve werking van interne beheersingsmaatregelen te toetsen, dient hij het interne beheersingsrisico in te schatten. Als de auditor niet van plan is om de effectieve werking van interne beheersingsmaatregelen te toetsen, dient zijn inschatting van het interne beheersingsrisico zodanig te zijn dat de inschatting van het risico op een afwijking van materieel belang hetzelfde is als de inschatting van inherent risico. (Zie par. A226-A229)

Evalueren van de controle-informatie verkregen uit de risico-inschattingswerkzaamheden

35. De auditor dient te evalueren of de controle-informatie verkregen uit de risico-inschattingswerkzaamheden een geschikte basis verschaft voor de identificatie en inschatting van de risico's op een afwijking van materieel belang. Zo niet, dan dient de auditor aanvullende risico-inschattingswerkzaamheden uit te voeren totdat controle-informatie is verkregen om een dergelijke basis te verschaffen. Bij het identificeren en inschatten van de risico's op een afwijking van materieel belang, dient de auditor rekening te houden met alle controle-informatie verkregen uit de risico-inschattingswerkzaamheden, hetzij bevestigend of tegenstrijdig met beweringen van het management. (Zie par. A230-A232)

Transactiestromen, rekeningsaldi en toelichtingen die niet significant zijn, maar die wel van materieel belang zijn

36. Voor van materieel belang zijnde transactiestromen, rekeningsaldi of toelichtingen die niet als significante transactiestromen, rekeningsaldi of toelichtingen zijn vastgesteld, dient de auditor te evalueren of deze vaststelling geschikt blijft. (Zie par. A233-A235)

Herziening van de risico-inschatting

37. Als de auditor nieuwe informatie verkrijgt die niet consistent is met de controle-informatie waarop de auditor oorspronkelijk de identificatie of inschattingen van de risico's op een afwijking van materieel belang baseerde, dient de auditor de identificatie of inschatting te herzien. (Zie par. A236)

Documentatie

38. De auditor dient in de controledocumentatie op te nemen:[13] (Zie par. A237-A241)

    (a) De bespreking tussen het opdrachtteam en de significante beslissingen die zijn genomen;
    (b) De belangrijke elementen van het verworven inzicht van de auditor in overeenstemming met paragrafen 19, 21, 22, 24 en 25; de informatiebronnen waaruit het inzicht van de auditor is verkregen; en de uitgevoerde risico-inschattingswerkzaamheden;
    (c) De evaluatie van de opzet van geïdentificeerde interne beheersingsmaatregelen, en de bepaling of dergelijke interne beheersingsmaatregelen geïmplementeerd zijn in overeenstemming met de vereisten in paragraaf 26; en
    (d) De geïdentificeerde en ingeschatte risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het niveau van beweringen, inclusief significante risico's en risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie kunnen verschaffen, en de beweegreden voor de significante oordeelsvormingen die gemaakt zijn.

****

[13] ISA 230, *Controledocumentatie*, paragrafen 8-11 en A6-A7.

Toepassingsgerichte en overige verklarende teksten

Definities (Zie par. 12)

Beweringen (Zie par. 12(a))

A1. Categorieën van beweringen worden bij het identificeren, inschatten en inspelen op de risico's op een afwijking van materieel belang door auditors gebruikt om de verschillende soorten potentiële afwijkingen van materieel belang die kunnen voorkomen te overwegen. Voorbeelden van deze categorieën beweringen worden beschreven in paragraaf A190. De beweringen verschillen van de schriftelijke bevestigingen vereist door ISA 580[14] om bepaalde aangelegenheden te bevestigen of andere controle-informatie te ondersteunen.

Interne beheersingsmaatregelen (Zie par. 12(c))

A2. Interne beheersingsmaatregelen zijn ingebed in de componenten van het interne beheersingssysteem van de entiteit.

A3. Beleidslijnen worden geïmplementeerd door de handelingen van het personeel binnen de entiteit, of door de terughoudendheid van het personeel om handelingen te ondernemen die in strijd zouden zijn met dergelijke beleidslijnen.

A4. Procedures kunnen verplicht worden gesteld door formele documentatie of andere communicatie door het management of de met governance belaste personen, of kunnen het gevolg zijn van gedragingen die niet verplicht zijn maar eerder bepaald worden door de cultuur van de entiteit. Procedures kunnen worden afgedwongen door de acties die worden toegestaan door de door de entiteit gebruikte IT-applicaties of andere aspecten van de IT-omgeving van de entiteit.

A5. Interne beheersingsmaatregelen kunnen direct of indirect zijn. Directe interne beheersingsmaatregelen zijn interne beheersingsmaatregelen die nauwkeurig genoeg zijn om in te spelen op risico's op een afwijking van materieel belang op het niveau van beweringen. Indirecte interne beheersingsmaatregelen zijn interne beheersingsmaatregelen die directe interne beheersingsmaatregelen ondersteunen.

Interne beheersingsmaatregelen voor informatieverwerking (Zie par. 12(e))

A6. Risico's voor de integriteit van informatie komen voort uit vatbaarheid voor een ineffectieve implementatie van de informatiebeleidslijnen van de entiteit; dit zijn beleidslijnen die de informatiestromen, vastleggingen en processen inzake financiële verslaggeving in het informatiesysteem van de entiteit definiëren. Interne beheersingsmaatregelen voor informatieverwerking zijn procedures die effectieve implementatie van de informatiebeleidslijnen van de entiteit ondersteunen. Interne beheersingsmaatregelen voor informatieverwerking kunnen geautomatiseerd zijn (d.w.z. ingebed in IT-applicaties) of handmatig (bijvoorbeeld interne beheersingsmaatregelen over invoer- of uitvoer) en kunnen steunen op andere interne beheersingsmaatregelen, waaronder die voor informatieverwerking of *general IT controls*.

Inherente risicofactoren (Zie par. 12(f))

Bijlage 2 bevat verdere overwegingen met betrekking tot het verwerven van inzicht in inherente risicofactoren.

A7. Inherente risicofactoren kunnen kwalitatief of kwantitatief zijn en de vatbaarheid van beweringen voor afwijkingen beïnvloeden. Kwalitatieve inherente risicofactoren met betrekking tot het opstellen van informatie vereist door het van toepassing zijnde stelsel inzake financiële verslaggeving omvatten:

[14] ISA 580, *Schriftelijke bevestigingen.*

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

- complexiteit;
- subjectiviteit;
- wijzigingen;
- onzekerheid; of
- vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of andere frauderisicofactoren voor zover ze het inherente risico beïnvloeden.

A8. Andere inherente risicofactoren, die van invloed zijn op de vatbaarheid van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting voor een afwijking kunnen omvatten:

- de kwantitatieve of kwalitatieve significantie van de transactiestroom, rekeningsaldo of toelichting; of
- de hoeveelheid of een gebrek aan uniformiteit in de samenstelling van de elementen die moeten worden verwerkt via de transactiestroom of het rekeningsaldo, of weergegeven in de toelichting.

Relevante beweringen (Zie par. 12(h))

A9. Een risico op een afwijking van materieel belang kan betrekking hebben op meer dan één bewering, in welk geval alle beweringen waarop een dergelijk risico betrekking heeft, relevante beweringen zijn. Als een bewering geen geïdentificeerd risico heeft op een afwijking van materieel belang, dan is het geen relevante bewering.

Significant risico (Zie par. 12(l))

A10. Significantie kan worden omschreven als het relatieve belang van een aangelegenheid en wordt ingeschat door de auditor in de context waarin de aangelegenheid wordt overwogen. Significantie kan worden overwogen door na te gaan in hoeverre inherente risicofactoren van invloed zijn op de waarschijnlijkheid dat een afwijking voorkomt en de orde van grootte van de potentiële afwijking indien die afwijking zou voorkomen.

Risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden (Zie par. 13-18)

A11. De risico's op een afwijking van materieel belang die moeten worden geïdentificeerd en ingeschat, omvatten zowel die het gevolg zijn van fraude als die welke het gevolg zijn van fouten en beide worden in deze ISA behandeld. De significantie van fraude is echter zodanig dat verdere vereisten en leidraden zijn opgenomen in ISA 240 met betrekking tot risico-inschattingswerkzaamheden en daarmee verband houdende werkzaamheden om informatie te verkrijgen die wordt gebruikt om de risico's op een afwijking van materieel belang als gevolg van fraude te identificeren en in te schatten.[15] Bovendien bieden de volgende ISA's nadere vereisten en leidraden voor het identificeren en inschatten van risico's op een afwijking van materieel belang met betrekking tot specifieke aangelegenheden of omstandigheden:

- ISA 540 (herzien) [16] met betrekking tot schattingen;
- ISA 550 met betrekking tot relaties en transacties met verbonden partijen;
- ISA 570 (herzien) [17] met betrekking tot continuïteit; en
- ISA 600 (herzien) [18] met betrekking tot financiële overzichten van de groep.

[15] ISA 240, paragrafen 12-27.
[16] ISA 540 (herzien), *De controle van schattingen en toelichtingen daarop.*
[17] ISA 570 (herzien), *Continuïteit.*
[18] ISA 600 (herzien), *Bijzondere overwegingen - Controles van financiële overzichten van de groep (inclusief het werk van groepsauditors).*

A12. Een professioneel-kritische instelling is noodzakelijk voor de kritische evaluatie van verzamelde controle-informatie bij het uitvoeren van de risico-inschattingswerkzaamheden. Deze instelling helpt de auditor alert te blijven voor controle informatie die niet tendeert naar het bevestigen van het bestaan van risico's of die tegenstrijdig kan zijn met het bestaan van risico's. Een professioneel-kritische instelling is een houding die door de auditor wordt toegepast wanneer professionele oordeelsvormingen worden gemaakt die vervolgens de basis vormen voor de handelingen van de auditor. De auditor past professionele oordeelsvorming toe bij het bepalen wanneer de auditor controle-informatie heeft die een geschikte basis verschaft voor risico-inschatting.

A13. De toepassing van een professioneel-kritische instelling door de auditor kan omvatten:

- tegenstrijdige informatie en de betrouwbaarheid van documenten ter discussie stellen;
- overwegen van reacties op verzoeken om inlichtingen en andere informatie verkregen van het management en de met governance belaste personen;
- alert zijn op omstandigheden die kunnen wijzen op mogelijke afwijking als gevolg van fraude of fouten; en
- overwegen of de verkregen controle-informatie de identificatie en inschatting van de risico's op een afwijking van materieel belang van de auditor ondersteunt in het licht van de aard en omstandigheden van de entiteit.

Waarom het verkrijgen van controle-informatie op een niet-tendentieuze manier belangrijk is (Zie par. 13)

A14. Het opzetten en uitvoeren van risico-inschattingswerkzaamheden om controle-informatie te verkrijgen ter ondersteuning van de identificatie en inschatting van de risico's op een afwijking van materieel belang op een niet-tendentieuze manier kan de auditor helpen bij het identificeren van mogelijk tegenstrijdige informatie. Die informatie kan de auditor helpen bij het uitoefenen van een professioneel-kritische instelling bij het identificeren en inschatten van de risico's op een afwijking van materieel belang.

Bronnen van controle-informatie (Zie par. 13)

A15. Risico-inschattingswerkzaamheden opzetten en uitvoeren om op een niet tendentieuze manier controle-informatie te verkrijgen kan bestaan uit het verkrijgen van informatie uit meerdere bronnen binnen en buiten de entiteit. De auditor hoeft echter niet een volledige zoekopdracht uit te voeren om alle mogelijke bronnen van controle-informatie te identificeren. Naast informatie uit andere bronnen[19], kunnen informatiebronnen voor risico-inschattingswerkzaamheden omvatten:

- interacties met het management, de met governance belaste personen en ander personeel van de entiteit op sleutelposities, zoals interne auditors;
- bepaalde externe partijen zoals regelgevers of toezichthouders, ongeacht of deze direct of indirect zijn verkregen;
- openbaar beschikbare informatie over de entiteit, bijvoorbeeld door de entiteit uitgegeven persberichten, materialen voor analisten of vergaderingen van investeerdersgroepen, analistenrapporten of informatie over handelsactiviteit.

Ongeacht de informatiebron houdt de auditor rekening met de relevantie en betrouwbaarheid van de informatie die moet worden gebruikt als controle-informatie in overeenstemming met ISA 500.[20]

Schaalbaarheid (Zie par. 13)

[19] Zie de paragrafen A37-A38.
[20] ISA 500, *Controle-informatie*, paragraaf 7.

A16. De aard en omvang van risico-inschattingswerkzaamheden zullen variëren op basis van de aard en omstandigheden van de entiteit (bijvoorbeeld mate waarin de beleidslijnen, procedures, processen en systemen van de entiteit geformaliseerd zijn). De auditor past professionele oordeelsvorming toe om de aard en omvang van de risico-inschattingswerkzaamheden die moeten worden uitgevoerd om aan de vereisten van deze ISA te voldoen, te bepalen.

A17. Hoewel de mate waarin de beleidslijnen, procedures, processen en systemen van een entiteit zijn geformaliseerd kan variëren, wordt van de auditor nog steeds vereist om het inzicht te verwerven in overeenstemming met paragrafen 19-22 en 24-26.

Voorbeelden:
Sommige entiteiten, waaronder minder complexe entiteiten, en met name door de eigenaar bestuurde entiteiten, hebben wellicht geen gestructureerde processen en systemen opgezet (bijvoorbeeld een risico-inschattingsproces of een proces om het systeem van interne beheersing te monitoren) of hebben mogelijk processen of systemen vastgesteld met beperkte documentatie of gebrek aan consistentie bij de uitvoering. Ook wanneer in dergelijke systemen en processen formalisering ontbreekt, kan de auditor nog steeds risico-inschattingswerkzaamheden uitvoeren door waarneming en verzoek om inlichtingen.

Van andere, doorgaans complexere entiteiten, wordt verwacht dat ze meer geformaliseerde en gedocumenteerde beleidslijnen en procedures hebben. De auditor kan dergelijke documentatie gebruiken bij het uitvoeren van risico-inschattingswerkzaamheden.

A18. De aard en omvang van risico-inschattingswerkzaamheden die moeten worden uitgevoerd bij de eerste keer dat een opdracht wordt uitgevoerd, kunnen uitgebreider zijn dan werkzaamheden voor een doorlopende opdracht. In opvolgende verslagperiodes kan de auditor zich richten op veranderingen die zich sinds de voorgaande verslagperiode hebben voorgedaan.

Soorten risico-inschattingswerkzaamheden (Zie par. 14)

A19. ISA 500 [21] legt de soorten controlewerkzaamheden uit die kunnen worden uitgevoerd bij het verkrijgen van controle-informatie van risico-inschattingswerkzaamheden en verdere controlewerkzaamheden. De aard, timing en omvang van de controlewerkzaamheden kunnen worden beïnvloed door het feit dat sommige van de administratieve gegevens en andere informatie mogelijk alleen beschikbaar zijn in elektronische vorm of alleen op bepaalde tijdstippen.[22] De auditor kan gegevensgerichte controles of toetsingen van interne beheersingsmaatregelen uitvoeren, in overeenstemming met ISA 330, gelijktijdig met risico inschattingswerkzaamheden wanneer dit efficiënt is om te doen. Verkregen controle-informatie die de identificatie en inschatting van risico's op een afwijking van materieel belang ondersteunt kan ook de detectie van afwijkingen op het niveau van beweringen of de evaluatie van de effectieve werking van interne beheersingsmaatregelen ondersteunen.

A20. Hoewel van de auditor vereist wordt om alle in paragraaf 14 beschreven risico-inschattingswerkzaamheden uit te voeren bij het verwerven van het vereiste inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit (Zie par. 19-26), wordt van de auditor niet vereist om ze allemaal uit te voeren voor elk aspect van dat inzicht. Andere werkzaamheden kunnen worden uitgevoerd wanneer de te verkrijgen informatie nuttig kan zijn bij het identificeren van risico's op afwijkingen van materieel belang. Voorbeelden van dergelijke werkzaamheden kunnen het verzoeken om inlichtingen zijn bij de externe juridisch adviseur of externe toezichthouders van de entiteit, of van waarderingsdeskundigen die de entiteit heeft gebruikt.

Geautomatiseerde hulpmiddelen en technieken (Zie par. 14)

[21] ISA 500, paragrafen A14-A17 en A21-A25.
[22] ISA 500, paragraaf A16.

A21. Gebruikmakend van geautomatiseerde hulpmiddelen en technieken, kan de auditor algemene risico-inschattingswerkzaamheden uitvoeren op grote aantallen gegevens (van het grootboek, subgrootboeken of andere operationele gegevens) alsmede voor analyse, herberekeningen, opnieuw uitvoeren of aansluitingen.

Verzoeken om inlichtingen bij het management en anderen binnen de entiteit (Zie par. 14(a))

Waarom verzoeken om inlichtingen worden gedaan bij het management en anderen binnen de entiteit

A22. Informatie verkregen door de auditor ter ondersteuning van een geschikte basis voor de identificatie en inschatting van risico's en het opzetten van verdere controlewerkzaamheden, kan worden verkregen door middel van verzoeken om inlichtingen bij het management en degenen die verantwoordelijk zijn voor financiële verslaggeving.

A23. Verzoeken om inlichtingen bij het management, degenen die verantwoordelijk zijn voor de financiële verslaggeving, andere geschikte personen binnen de entiteit en andere werknemers met verschillende beslissingsbevoegdheden kunnen de auditor verschillende perspectieven bieden bij het identificeren en inschatten van risico's op een afwijking van materieel belang.

Voorbeelden:

- Verzoeken om inlichtingen gericht aan de met governance belaste personen kunnen de auditor helpen inzicht te verwerven in de mate van toezicht door de met governance belaste personen op het opstellen van de financiële overzichten door het management. ISA 260 [23] onderkent het belang van effectieve wederzijdse communicatie om de auditor te helpen in dit verband informatie te verkrijgen van de met governance belaste personen.
- Verzoeken om inlichtingen bij werknemers die verantwoordelijk zijn voor het initiëren, verwerken of vastleggen van complexe of ongebruikelijke transacties kunnen de auditor helpen bij het evalueren in welke mate de keuze en toepassing van bepaalde grondslagen voor financiële verslaggeving passend zijn.
- Verzoeken om inlichtingen bij de interne juridische adviseur kunnen informatie verstrekken over aangelegenheden als rechtszaken, de naleving van wet- en regelgeving, kennis van fraude of vermoede fraude die de entiteit beïnvloedt, garanties, verplichtingen na verkoop, overeenkomsten (zoals joint ventures) met zakenpartners en de betekenis van contractuele bepalingen.
- Verzoeken om inlichtingen bij marketing- of verkooppersoneel kunnen informatie verschaffen over wijzigingen in de marketingstrategieën van de entiteit, verkooptrends of contractuele overeenkomsten met haar klanten.
- Verzoeken om inlichtingen gericht op de risicomanagementfunctie (of verzoeken om inlichtingen aan personen die dergelijke rollen uitvoeren) kunnen informatie verschaffen over operationele en wettelijke risico's die van invloed kunnen zijn op de financiële verslaggeving.
- Verzoeken om inlichtingen gericht aan IT-personeel kunnen informatie verschaffen over systeemwijzigingen, falen van systeem- of interne beheersing, of andere IT-gerelateerde risico's.

Overwegingen specifiek voor entiteiten in de publieke sector

A24. Bij verzoeken om inlichtingen bij personen die informatie kunnen hebben die waarschijnlijk zal helpen bij het identificeren van risico's op een afwijking van materieel belang, kunnen auditors van entiteiten in de publieke sector informatie verkrijgen van aanvullende informatiebronnen zoals van de auditors die betrokken zijn bij doelmatigheids- of andere controles met betrekking tot de entiteit.

Verzoeken om inlichtingen bij de interne auditfunctie

[23] ISA 260 (herzien), *Communicatie met de met governance belaste personen*, paragraaf 4(b).

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

Bijlage 4 bevat overwegingen voor het verwerven van inzicht in de interne auditfunctie van een entiteit.

Waarom verzoeken om inlichtingen worden gesteld bij de interne auditfunctie (als de functie bestaat)

A25. Als een entiteit een interne auditfunctie heeft, kunnen verzoeken om inlichtingen bij de juiste personen binnen de functie de auditor helpen bij het verwerven van inzicht in de entiteit en haar omgeving en het systeem van interne beheersing van de entiteit bij het identificeren en inschatten van risico's.

Overwegingen specifiek voor entiteiten in de publieke sector

A26. Auditors van entiteiten in de publieke sector hebben vaak extra verantwoordelijkheden met betrekking tot interne beheersing en naleving van de van toepassing zijnde wet- en regelgeving. Verzoeken om inlichtingen bij geschikte personen in de interne auditfunctie kunnen de auditors helpen bij het identificeren van het risico op niet-naleving van de van toepassing zijnde wet- en regelgeving van materieel belang en het risico op tekortkomingen in de interne beheersing met betrekking tot financiële verslaggeving.

Cijferanalyses (Zie par. 14(b))

Waarom cijferanalyses worden uitgevoerd als een van de risico-inschattingswerkzaamheden

A27. Cijferanalyses helpen bij het identificeren van inconsistenties, ongebruikelijke transacties of gebeurtenissen, bedragen, ratio's en trends die wijzen op aangelegenheden die implicaties voor de controle kunnen hebben. Ongebruikelijke of onverwachte relaties die geïdentificeerd zijn, kunnen de auditor helpen bij het identificeren van risico's op een afwijking van materieel belang; met name risico's op een afwijking van materieel belang als gevolg van fraude.

A28. Cijferanalyses die worden uitgevoerd als risico-inschattingswerkzaamheden kunnen daarom helpen bij het identificeren en het inschatten van de risico's op een afwijking van materieel belang door aspecten van de entiteit te identificeren waarvan de auditor zich niet bewust van was of niet begreep hoe inherente risicofactoren, zoals wijzigingen, de vatbaarheid van beweringen voor afwijkingen beïnvloeden.

Soorten cijferanalyses

A29. Cijferanalyses uitgevoerd als risico-inschattingswerkzaamheden kunnen:

- zowel financiële als niet-financiële informatie omvatten, bijvoorbeeld de relatie tussen verkoop en vierkante meters van verkoopruimte of hoeveelheid verkochte goederen (niet-financieel);
- gegevens gebruiken die op een hoog niveau zijn samengevoegd. Dienovereenkomstig kunnen de resultaten van die cijferanalyses een eerste globale indicatie geven van de waarschijnlijkheid van een afwijking van materieel belang.

Voorbeeld:
Bij de controle van veel entiteiten, waaronder die met minder complexe bedrijfsmodellen en processen en een minder complex informatiesysteem, kan de auditor een eenvoudige vergelijking van informatie uitvoeren, zoals de wijziging in tussentijdse of maandelijkse rekeningsaldi ten opzichte van saldi in eerdere verslagperiodes om een indicatie te krijgen van mogelijk hogere risicogebieden.

A30. Deze ISA behandelt het gebruik door de auditor van cijferanalyses als risico-inschattingswerkzaamheden. ISA 520[24] behandelt het gebruik door de auditor van cijferanalyses als gegevensgerichte werkzaamheden ('gegevensgerichte' cijferanalyses') en de

[24] ISA 520, *Cijferanalyses.*

verantwoordelijkheid van de auditor om cijferanalyses nabij het einde van de controle uit te voeren. Dienovereenkomstig is het niet vereist om cijferanalyses die worden uitgevoerd als risico-inschattingswerkzaamheden uit te voeren in overeenstemming met de vereisten van ISA 520. Echter, de vereisten en toepassingsgerichte teksten in ISA 520 kunnen bruikbare leidraden bieden aan de auditor bij het uitvoeren cijferanalyses als onderdeel van de risico-inschattingswerkzaamheden.

Geautomatiseerde hulpmiddelen en technieken

A31. Cijferanalyses kunnen worden uitgevoerd met behulp van een aantal hulpmiddelen of technieken, die geautomatiseerd kunnen zijn. Het toepassen van geautomatiseerde cijferanalyses op de gegevens kan worden aangeduid als data analyse.

Voorbeeld:
De auditor kan een spreadsheet gebruiken om een vergelijking te maken van de werkelijk vastgelegde bedragen ten opzichte van gebudgetteerde bedragen, of kan een meer geavanceerde maatregel uitvoeren door gegevens uit het informatiesysteem van de entiteit te extraheren en deze gegevens verder analyseren met behulp van visualisatietechnieken om transactiestromen, rekeningsaldi of toelichtingen te identificeren waarvoor verdere specifieke risico-inschattingswerkzaamheden gerechtvaardigd kunnen zijn.

Waarneming en inspectie (Zie par. 14(c))

Waarom waarneming en inspectie worden uitgevoerd als risico-inschattingswerkzaamheden

A32. Waarneming en inspectie kunnen verzoeken om inlichtingen bij het management en anderen ondersteunen, bevestigen of tegenspreken en kunnen ook informatie verschaffen over de entiteit en haar omgeving.

Schaalbaarheid

A33. Wanneer beleidslijnen of procedures niet zijn gedocumenteerd of de entiteit minder geformaliseerde interne beheersingsmaatregelen heeft, kan de auditor nog steeds enige controle-informatie verkrijgen om de identificatie en inschatting van de risico's op een afwijking van materieel belang te ondersteunen door waarneming of inspectie van de uitvoering van de interne beheersingsmaatregel.

Voorbeelden:
- De auditor kan inzicht verwerven in de interne beheersingsmaatregelen met betrekking tot een voorraadopname, zelfs als deze niet door de entiteit zijn gedocumenteerd, door directe waarneming.
- De auditor kan in staat zijn functiescheiding waar te nemen.
- De auditor kan in staat zijn waar te nemen dat wachtwoorden worden ingevoerd.

Waarneming en inspectie als risico-inschattingswerkzaamheden

A34. Risico-inschattingswerkzaamheden kunnen waarneming of inspectie van het volgende omvatten:

- de activiteiten van de entiteit;
- interne documenten (zoals ondernemingsplannen en strategieën), vastleggingen en handboeken over de interne beheersing;
- verslagen opgesteld door het management (zoals kwartaalverslagen van het management en tussentijdse financiële overzichten) en de met governance belaste personen (zoals notulen van de vergaderingen van de raad van bestuur);
- de panden en fabrieksinstallaties van de entiteit;
- informatie verkregen uit externe bronnen zoals handels- en economische tijdschriften; rapporten door analisten, banken of kredietbeoordelaars; publicaties van regelgevende of

toezichthoudende instanties of financiële publicaties; of andere externe documenten over de financiële prestaties van de entiteit (zoals die waarnaar in paragraaf A79 wordt verwezen);
- de gedragingen en de handelingen van het management of de met governance belaste personen (zoals de waarneming van een vergadering van het auditcomité).

Geautomatiseerde hulpmiddelen en technieken

A35. Geautomatiseerde hulpmiddelen of technieken kunnen ook worden gebruikt om waar te nemen of te inspecteren, in het bijzonder activa, bijvoorbeeld door het gebruik van externe waarnemingshulpmiddelen (bijv. een drone).

Overwegingen specifiek voor entiteiten in de publieke sector

A36. Risico-inschattingswerkzaamheden die worden uitgevoerd door auditors van entiteiten in de publieke sector kunnen ook waarneming en inspectie van documenten opgesteld door het management voor de wetgever omvatten, bijvoorbeeld documenten met betrekking tot verplichte rapportage van prestaties.

Informatie uit andere bronnen (Zie par. 15)

Waarom de auditor informatie uit andere bronnen overweegt

A37. Informatie verkregen uit andere bronnen kan relevant zijn voor de identificatie en inschatting van de risico's op een afwijking van materieel belang door het verstrekken van informatie en inzichten over:

- de aard van de entiteit en haar bedrijfsrisico's en wat gewijzigd kan zijn ten opzichte van de vorige verslagperiodes;
- de integriteit en ethische waarden van het management en de met governance belaste personen, die ook relevant kunnen zijn voor het inzicht van de auditor in de interne beheersingsomgeving;
- het van toepassing zijnde stelsel inzake financiële verslaggeving en de toepassing ervan op de aard en omstandigheden van de entiteit.

Andere relevante bronnen

A38. Andere relevante informatiebronnen omvatten:

- de werkzaamheden van de auditor met betrekking tot aanvaarding of continuering van de cliëntrelatie of de controleopdracht in overeenstemming met ISA 220 (herzien), inclusief de conclusies die hierover zijn getrokken;[25]
- andere opdrachten voor de entiteit die door de opdrachtpartner zijn uitgevoerd. De opdrachtpartner kan kennis hebben verkregen die relevant is voor de controle, inclusief kennis over de entiteit en haar omgeving bij het uitvoeren van andere opdrachten voor de entiteit. Dergelijke opdrachten kunnen opdrachten tot het uitvoeren van overeengekomen specifieke werkzaamheden of andere controle- of assurance-opdrachten omvatten, inclusief opdrachten om te voldoen aan incrementele verslaggevingsvereisten in het rechtsgebied.

Informatie uit eerdere ervaringen van de auditor met de entiteit en eerdere controles (Zie par. 16)

Waarom informatie uit eerdere controles belangrijk is voor de lopende controle

[25] ISA 220 (herzien), *Kwaliteitsmanagement voor een controle van financiële overzichten*, paragraaf 22-24.

A39. De eerdere ervaring van de auditor met de entiteit en uit controlewerkzaamheden die zijn uitgevoerd in eerdere controles kunnen de auditor informatie verschaffen die relevant is voor de bepaling door de auditor van de aard en omvang van risico-inschattingswerkzaamheden en de identificatie en inschatting van risico's op afwijkingen van materieel belang.

Aard van de informatie uit eerdere controles

A40. De eerdere ervaring van de auditor met de entiteit en controlewerkzaamheden die zijn uitgevoerd bij eerdere controles kan de auditor informatie verstrekken over aangelegenheden als:

- afwijkingen uit het verleden en of deze tijdig zijn gecorrigeerd;
- de aard van de entiteit en haar omgeving en het systeem van interne beheersing van de entiteit (inclusief tekortkomingen in de interne beheersing);
- significante wijzigingen die de entiteit of haar activiteiten sinds de vorige financiële verslagperiode hebben ondergaan;
- die bijzondere soorten transacties en andere gebeurtenissen of rekeningsaldi (en daarmee samenhangende toelichtingen) waar de auditor moeilijkheden ondervond bij met het uitvoeren van de noodzakelijke controlewerkzaamheden, bijvoorbeeld vanwege hun complexiteit.

A41. Van de auditor wordt vereist om te bepalen of informatie verkregen uit de vorige ervaring van de auditor met de entiteit en van controlewerkzaamheden die bij eerdere controles zijn uitgevoerd, relevant en betrouwbaar blijft, als de auditor voornemens is die informatie te gebruiken voor de doeleinden van de lopende controle. Als de aard of omstandigheden van de entiteit zijn gewijzigd of nieuwe informatie is verkregen, is de informatie uit voorgaande verslagperioden mogelijk niet langer relevant of betrouwbaar voor de lopende controle. Om te bepalen of er wijzigingen zijn voorgekomen die de relevantie of betrouwbaarheid van dergelijke informatie kunnen beïnvloeden, kan de auditor verzoeken om inlichtingen en andere geschikte controlewerkzaamheden uitvoeren, zoals lijncontroles van relevante systemen. Als de informatie niet betrouwbaar is, kan de auditor overwegen extra werkzaamheden uit te voeren die passend zijn in de omstandigheden.

Bespreking opdrachtteam (Zie par. 17-18)

Waarom het opdrachtteam de toepassing van het van toepassing zijnde stelsel inzake financiële verslaggeving en de vatbaarheid van de financiële overzichten van de entiteit voor afwijkingen van materieel belang moet bespreken

A42. De bespreking binnen het opdrachtteam over de toepassing van het van toepassing zijnde stelsel inzake financiële verslaggeving en de vatbaarheid van de financiële overzichten van de entiteit voor afwijkingen van materieel belang:

- biedt een kans voor meer ervaren leden van het opdrachtteam, waaronder de opdrachtpartner, om de op hun kennis van de entiteit gebaseerde inzichten te delen. Het delen van informatie draagt bij aan een verbeterd inzicht door alle leden van het opdrachtteam;
- staat de opdrachtteamleden toe om informatie uit te wisselen over de bedrijfsrisico's waaraan de entiteit is blootgesteld, hoe inherente risicofactoren de vatbaarheid voor afwijkingen van transactiestromen, rekeningsaldi en toelichtingen kunnen beïnvloeden en over hoe en waar de financiële overzichten vatbaar kunnen zijn voor een afwijking van materieel belang als gevolg van fraude of fouten;
- helpt de betrokken teamleden om een beter inzicht te krijgen in de mogelijkheid voor een afwijking van materieel belang in de financiële overzichten in de specifieke gebieden die aan hen zijn toegewezen en om inzicht te verwerven in hoe de resultaten van de door hen uitgevoerde controlewerkzaamheden van invloed kunnen zijn op andere aspecten van de controle, inclusief de beslissingen over de aard, timing en omvang van verdere controlewerkzaamheden. De bespreking helpt van het opdrachtteam in het bijzonder

tegenstrijdige informatie verder te overwegen op basis van het eigen inzicht van elk lid in de aard en omstandigheden van de entiteit;
- biedt een basis waarop leden van het opdrachtteam nieuwe informatie verkregen tijdens de controle en die van invloed kan zijn op de inschatting van risico's op een afwijking van materieel belang of op de uitgevoerde controlewerkzaamheden om in te spelen op deze risico's communiceren en delen.

ISA 240 vereist dat de opdrachtteam bespreking bijzondere nadruk legt op hoe en waar de financiële overzichten van de entiteit mogelijk vatbaar zijn voor afwijkingen van materieel belang als gevolg van fraude, waaronder hoe fraude kan voorkomen.[26]

A43. Een professioneel-kritische instelling is noodzakelijk voor de kritische inschatting van controle-informatie en een robuuste en open opdrachtteam bespreking, ook voor doorlopende controles, kan leiden tot verbeterde identificatie en inschatting van de risico's op een afwijking van materieel belang. Een ander resultaat van de bespreking kan zijn dat de auditor specifieke gebieden van de controle identificeert waarvoor het uitoefenen van een professioneel-kritische instelling bijzonder belangrijk is en wat kan leiden tot de betrokkenheid van meer ervaren leden van het opdrachtteam die voldoende bekwaam zijn om betrokken te zijn bij de uitvoering van controlewerkzaamheden met betrekking tot deze gebieden.

Schaalbaarheid

A44. Wanneer de opdracht wordt uitgevoerd door een enkele persoon, zoals een zelfstandige auditor (d.w.z. waar een opdrachtteam bespreking niet mogelijk is), kan overweging van de in de paragrafen A42 en A46 genoemde aangelegenheden de auditor niettemin helpen om te identificeren waar er risico's kunnen zijn op afwijkingen van materieel belang.

A45. Wanneer een opdracht wordt uitgevoerd door een groot opdrachtteam, zoals voor een controle van financiële overzichten van de groep, is het niet altijd noodzakelijk of praktisch uitvoerbaar dat de bespreking alle leden in een enkele bespreking omvat (bijvoorbeeld in een controle die meerdere locaties betreft), noch is het nodig dat alle leden van het opdrachtteam op de hoogte worden gehouden van alle beslissingen die in de bespreking zijn genomen. De opdrachtpartner kan aangelegenheden bespreken met kernleden van het opdrachtteam, met inbegrip van, indien nodig geacht, degenen met specifieke vaardigheden of kennis en degenen die verantwoordelijk zijn voor de werkzaamheden die moeten worden uitgevoerd bij groepsonderdelen, terwijl bespreking met anderen wordt gedelegeerd, rekening houdend met de omvang van communicatie die door het hele opdrachtteam noodzakelijk wordt geacht. Een door de opdrachtpartner goedgekeurd communicatieplan kan nuttig zijn.

Bespreking van toelichtingen in het van toepassing zijnde stelsel inzake financiële verslaggeving

A46. Als onderdeel van de bespreking binnen het opdrachtteam, helpt rekening houden met de toelichtingsvereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving in het begin van de controle bij het identificeren van mogelijke risico's op een afwijking van materieel belang met betrekking tot toelichtingen, zelfs in omstandigheden waarin het van toepassing zijnde stelsel inzake financiële verslaggeving alleen vereenvoudigde toelichtingen vereist. Aangelegenheden die het opdrachtteam kan bespreken omvatten:

- veranderingen in financiële verslaggevingsvereisten die kunnen leiden tot significante nieuwe of herziene toelichtingen;
- veranderingen in de omgeving, financiële toestand of activiteiten van de entiteit die kunnen leiden tot significante nieuwe of herziene toelichtingen, bijvoorbeeld een significante fusie of overname in de gecontroleerde verslagperiode;
- toelichtingen waarvoor het verkrijgen van voldoende en geschikte controle-informatie moeilijk kan zijn geweest in het verleden; en

[26] ISA 240, paragraaf 16.

- toelichtingen over complexe aangelegenheden, waaronder die waarbij significante oordeelsvorming van het management betrokken is over welke informatie moet worden toegelicht.

Overwegingen specifiek voor entiteiten in de publieke sector

A47. Als onderdeel van de bespreking binnen het opdrachtteam door auditors van entiteiten in de publieke sector, kan er ook rekening worden gehouden met eventuele aanvullende bredere doelstellingen en bijbehorende risico's die voortkomen uit het controlemandaat of verplichtingen voor entiteiten in de publieke sector.

Het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het systeem van interne beheersing van de entiteit (Zie par. 19-27)

In de **bijlagen 1 tot en met 6** worden verdere overwegingen uiteengezet met betrekking tot het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het systeem van interne beheersing van de entiteit.

Het verwerven van het vereiste inzicht (Zie par. 19-27)

A48. Het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit is een dynamisch en iteratief proces van verzamelen, bijwerken en analyseren van informatie en dit gaat door tijdens de controle. Daarom kunnen de verwachtingen van de auditor veranderen als nieuwe informatie wordt verkregen.

A49. Het inzicht van de auditor in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving kan de auditor ook helpen bij het ontwikkelen van initiële verwachtingen over de transactiestromen, rekeningsaldi en toelichtingen die significante transactiestroom, rekeningsaldi en toelichtingen kunnen zijn. Deze verwachte significante transactiestromen, rekeningsaldi en toelichtingen vormen de basis voor de reikwijdte van het inzicht van de auditor in het informatiesysteem van de entiteit.

Waarom inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving wordt vereist (Zie par. 19-20)

A50. Het inzicht van de auditor in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving, helpt de auditor bij het verwerven van inzicht in de gebeurtenissen en omstandigheden die relevant zijn voor de entiteit en bij het identificeren hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen bij het opstellen van de financiële overzichten beïnvloeden, in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving en de mate waarin zij dit doen. Dergelijke informatie vormt een referentiekader waarbinnen de auditor risico's op een afwijking van materieel belang identificeert en inschat. Dit referentiekader helpt de auditor ook bij het plannen van de controle en het uitoefenen van professionele oordeelsvorming en een professioneel-kritische instelling gedurende de gehele controle, bijvoorbeeld bij:

- het identificeren en inschatten van risico's op een afwijking van materieel belang in de financiële overzichten in overeenstemming met ISA 315 (herzien 2019) of andere relevante ISA's (bijv. met betrekking tot risico's op fraude in overeenstemming met ISA 240 of bij het identificeren of inschatten van risico's met betrekking tot schattingen in overeenstemming met ISA 540 (herzien);

- het uitvoeren van werkzaamheden om bij te dragen tot het identificeren van gevallen van niet-naleving van wet- en regelgeving die een invloed van materieel belang kunnen hebben op de financiële overzichten in overeenstemming met ISA 250 (herzien);[27]
- het evalueren of de financiële overzichten voldoende toelichtingen verschaffen in overeenstemming met ISA 700 (herzien) ;[28]
- het bepalen van materialiteit of uitvoeringsmaterialiteit in overeenstemming met ISA 320;[29] of
- het overwegen van de geschiktheid van de keuze en toepassing van grondslagen voor financiële verslaggeving en de toereikendheid van de toelichtingen bij de financiële overzichten.

A51. Het inzicht van de auditor in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving, is ook de basis voor de manier waarop de auditor verdere controlewerkzaamheden plant en uitvoert, bijvoorbeeld bij:

- het ontwikkelen van verwachtingen voor gebruik bij het uitvoeren van cijferanalyses in overeenstemming met ISA 520;[30]
- het opzetten en uitvoeren van verdere controlewerkzaamheden om voldoende en geschikte controle te verkrijgen in overeenstemming met ISA 330; en
- het evalueren van de toereikendheid en geschiktheid van verkregen controle-informatie (bijv. met betrekking tot veronderstellingen of mondelinge en schriftelijke bevestigingen van het management).

Schaalbaarheid

A52. De aard en omvang van het vereiste inzicht is een aangelegenheid van professionele oordeelsvorming door de auditor en varieert van entiteit tot entiteit gebaseerd op de aard en omstandigheden van de entiteit, waaronder:

- de omvang en complexiteit van de entiteit, inclusief haar IT-omgeving;
- de eerdere ervaring van de auditor met de entiteit;
- de aard van de systemen en processen van de entiteit, inclusief of deze al dan niet geformaliseerd zijn; en
- de aard en vorm van de documentatie van de entiteit.

A53. De risico-inschattingswerkzaamheden van de auditor om het vereiste inzicht te verwerven, kunnen minder uitgebreid zijn in controles van minder complexe entiteiten en uitgebreider voor complexere entiteiten. De diepte van het inzicht dat door de auditor wordt vereist, zal naar verwachting minder zijn dan het inzicht dat het management bezit bij het leiden van de entiteit.

A54. Sommige stelsels inzake financiële verslaggeving staan kleinere entiteiten toe om eenvoudigere en minder gedetailleerde toelichtingen te verschaffen in de financiële overzichten. Dit ontslaat de auditor echter niet van zijn verantwoordelijkheid om inzicht te verwerven in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving zoals het van toepassing is op de entiteit.

A55. Het gebruik van IT door de entiteit en de aard en omvang van veranderingen in de IT-omgeving kunnen ook van invloed zijn op de specialistische vaardigheden die nodig zijn om het vereiste inzicht te verwerven.

De entiteit en haar omgeving (Zie par. 19(a))

---

[27] ISA 250 (herzien), *Het in aanmerking nemen van wet- en regelgeving bij een controle van financiële overzichten*, paragraaf 14.
[28] ISA 700 (herzien), *Het vormen van een oordeel vormen en het rapporteren over financiële overzichten*, paragraaf 13(e).
[29] ISA 320, *Materialiteit bij het plannen en uitvoeren van een controle*, paragrafen 10-11.
[30] ISA 520, paragraaf 5.

De organisatiestructuur, het eigendom en de governance van de entiteit en het bedrijfsmodel (Zie par. 19(a)(i))

De organisatiestructuur en eigendom van de entiteit

A56. Inzicht in de organisatiestructuur en eigendom van de entiteit kan de auditor in staat stellen inzicht te verwerven in aangelegenheden als:

- De complexiteit van de structuur van de entiteit.

Voorbeeld:
De entiteit kan een enkele entiteit zijn of de structuur van de entiteit kan dochterondernemingen, divisies of andere groepsonderdelen op meerdere locaties omvatten. Verder kan de juridische structuur verschillen van de operationele structuur. Complexe structuren introduceren vaak factoren die aanleiding kunnen geven tot hogere vatbaarheid voor risico's op een afwijking van materieel belang. Dergelijke kwesties kunnen betrekking hebben op de vraag of goodwill, joint ventures, investeringen of voor een bijzonder doel opgerichte entiteiten op de juiste wijze administratief zijn verwerkt en of adequate toelichting van dergelijke kwesties is gegeven in de financiële overzichten.

- Het eigendom en relaties tussen eigenaren en andere mensen of entiteiten, inclusief verbonden partijen. Dit inzicht kan helpen om te bepalen of transacties met verbonden partijen op passende wijze zijn geïdentificeerd, verantwoord en voldoende toegelicht in de financiële overzichten.[31]
- Het onderscheid tussen de eigenaars, de met governance belaste personen en management.

Voorbeeld:
In minder complexe entiteiten kunnen eigenaren van de entiteit betrokken zijn bij het leiden van de entiteit, daarom is daar weinig of geen onderscheid. Daarentegen kan er een duidelijk onderscheid zijn tussen het management, de eigenaren van de entiteit en de met governance belaste personen zoals in sommige *oob's of andere beursgenoteerde entiteiten*.[32]

- De structuur en complexiteit van de IT-omgeving van de entiteit.

Voorbeelden:
Een entiteit kan:
- meerdere verouderde IT-systemen hebben in diverse bedrijfsactiviteiten die niet goed zijn geïntegreerd, resulterend in een complexe IT-omgeving.
- Gebruikmaken van externe of interne serviceproviders voor aspecten van zijn IT-omgeving (bijv. het uitbesteden van de *hosting* van zijn IT-omgeving aan een derde of een gedeeld servicecentrum voor centraal beheer van IT-processen in een groep).

Geautomatiseerde hulpmiddelen en technieken

A57. De auditor kan geautomatiseerde hulpmiddelen en technieken gebruiken om inzicht te verwerven in transactiestromen en verwerking als onderdeel van de werkzaamheden van de auditor om inzicht te verwerven in het informatiesysteem. Een uitkomst van deze werkzaamheden kan zijn dat de auditor informatie verkrijgt over de organisatiestructuur van de entiteit of degenen waarmee de entiteit zaken doet (bijvoorbeeld leveranciers, klanten, verbonden partijen).

Overwegingen specifiek voor entiteiten in de publieke sector

[31] ISA 550 stelt vereisten vast en geeft leidraden over de overwegingen van de auditor met betrekking tot verbonden partijen.
[32] ISA 260, paragrafen A1 en A2 bieden leidraden voor de identificatie van de met governance belaste personen en legt uit dat in sommige gevallen sommige of alle personen belast met governance betrokken kunnen zijn bij het leiden van de entiteit.

A58. Het eigendom van een entiteit in de publieke sector heeft mogelijk niet dezelfde relevantie als in de particuliere sector omdat als gevolg van politieke processen beslissingen met betrekking tot de entiteit buiten de entiteit kunnen worden genomen. Daarom heeft het management mogelijk geen zeggenschap over bepaalde beslissingen die worden genomen. Aangelegenheden die relevant kunnen zijn omvatten onder meer inzicht in de mogelijkheid van de entiteit om eenzijdige beslissingen te nemen en de mogelijkheid van andere entiteiten in de publieke sector om het mandaat en de strategische richting van de entiteit te beheersen of te beïnvloeden.

Voorbeeld:
Een entiteit in de publieke sector kan onderworpen zijn aan wetten of andere aanwijzingen van autoriteiten die dit vereisen om goedkeuring te krijgen van externe partijen van de entiteit van haar strategie en doelstellingen voorafgaand aan de implementatie daarvan. Daarom kunnen aangelegenheden met betrekking tot het verwerven van inzicht in de juridische structuur van de entiteit van toepassing zijnde wet- en regelgeving omvatten en de classificatie van de entiteit (d.w.z. of de entiteit een ministerie, departement agentschap of ander type entiteit is).

Governance

Waarom de auditor inzicht in de governance verkrijgt

A59. Inzicht in de governance van de entiteit kan de auditor helpen bij het verwerven van inzicht in de mogelijkheid van de entiteit om passend toezicht te houden op haar interne beheersingssysteem. Dit inzicht kan echter ook informatie verschaffen inzake tekortkomingen, wat kan wijzen op een toename van de vatbaarheid van de financiële overzichten van de entiteit voor risico's op afwijkingen van materieel belang.

Inzicht in de governance van de entiteit

A60. Aangelegenheden die relevant kunnen zijn voor de auditor om te overwegen bij het verwerven van inzicht in de governance van de entiteit omvatten:

- of een of meer van de met governance belaste personen betrokken zijn bij het leiden van de entiteit;
- het bestaan (en de scheiding) van een niet-dagelijks bestuur, indien aanwezig, van dagelijks bestuur;
- of de met governance belaste personen posities bekleden die een integraal onderdeel zijn van de juridische structuur van de entiteit, bijvoorbeeld als directeur;
- het bestaan van subgroepen van de met governance belaste personen, zoals een auditcomité, en de verantwoordelijkheden van een dergelijke groep;
- de verantwoordelijkheden van de met governance belaste personen voor het toezicht op de financiële verslaggeving, inclusief goedkeuring van de financiële overzichten.

Het bedrijfsmodel van de entiteit

Bijlage 1 bevat aanvullende overwegingen voor het verwerven van inzicht in de entiteit en haar bedrijfsmodel, evenals aanvullende overwegingen voor het controleren van voor een bijzonder doel opgerichte entiteiten.

Waarom de auditor inzicht krijgt in het bedrijfsmodel van de entiteit

A61. Inzicht in de doelstellingen, strategie en bedrijfsmodel van de entiteit helpt de auditor om inzicht te verwerven in de entiteit op strategisch niveau en om de bedrijfsrisico's te begrijpen die de entiteit neemt en loopt. Een inzicht in de bedrijfsrisico's die van invloed zijn op de financiële overzichten helpt de auditor bij het identificeren van risico's op een afwijking van materieel belang, aangezien de meeste bedrijfsrisico's uiteindelijk financiële consequenties hebben en derhalve een effect op de financiële overzichten.

Voorbeelden:
Het bedrijfsmodel van een entiteit kan op verschillende manieren steunen op het gebruik van IT:
- de entiteit verkoopt schoenen uit een fysieke winkel en gebruikt een geavanceerde voorraad- en kassasysteem om de verkoop van schoenen vast te leggen; of
- de entiteit verkoopt schoenen online zodat alle verkooptransacties in een IT omgeving worden verwerkt, inclusief het initiëren van de transacties via een website.

Voor beide entiteiten zouden de bedrijfsrisico's die voortkomen uit een significant ander bedrijfsmodel substantieel anders zijn, ondanks dat beide entiteiten schoenen verkopen.

Inzicht in het bedrijfsmodel van de entiteit

A62. Niet alle aspecten van het bedrijfsmodel zijn relevant voor het inzicht van de auditor. Bedrijfsrisico's zijn breder dan de risico's op een afwijking van materieel belang in de financiële overzichten, hoewel bedrijfsrisico's de laatste omvatten. De auditor heeft geen verantwoordelijkheid om inzicht te verwerven in alle bedrijfsrisico's of ze te identificeren omdat niet alle bedrijfsrisico's aanleiding geven tot risico's op een afwijking van materieel belang.

A63. Bedrijfsrisico's die de vatbaarheid voor risico's op een afwijking van materieel belang vergroten, kunnen voortkomen uit:

- ongeschikte doelstellingen of strategieën, ineffectieve uitvoering van strategieën, of wijzigingen of complexiteit;
- het niet onderkennen van de noodzaak voor wijzigingen, wat ook aanleiding kan geven tot bedrijfsrisico's bijvoorbeeld van:
    - de ontwikkeling van nieuwe producten of diensten die mogelijk geen succes zijn;
    - een markt die, zelfs als deze met goed gevolg is ontwikkeld, een product of dienst niet op adequate wijze ondersteunt; of
    - gebreken in een product of dienst tot wettelijke aansprakelijkheid en reputatierisico kunnen leiden.
- stimulansen en druk op het management, die kunnen resulteren in opzettelijke of onopzettelijke tendenties bij het management en die daarom de redelijkheid van significante veronderstellingen en de verwachtingen van het management of de met governance belaste personen beïnvloeden.

A64. Voorbeelden van aangelegenheden die de auditor kan overwegen bij het verkrijgen van inzicht in het bedrijfsmodel, doelstellingen, strategieën en gerelateerde bedrijfsrisico's van de entiteit die kunnen leiden tot een risico van materieel belang op afwijkingen van de financiële overzichten omvatten:

- ontwikkelingen in de sector, zoals het gebrek aan personeel of expertise om de veranderingen in de sector aan te pakken;
- nieuwe producten en diensten die kunnen leiden tot hogere productaansprakelijkheid;
- uitbreiding van de activiteiten van de entiteit, terwijl de vraag niet nauwkeurig is geschat;
- nieuwe voorschriften inzake administratieve verwerking bij onvolledige of onjuiste implementatie;
- vereisten op grond van regelgeving resulterend in een hogere juridische blootstelling;
- huidige en toekomstige financieringsbehoeften, zoals verlies van financiering doordat de entiteit niet in staat is haar verplichtingen na te komen;
- gebruik van IT, zoals de implementatie van een nieuw IT-systeem dat gevolgen heeft voor zowel de bedrijfsvoering als financiële verslaggeving; of
- de effecten van het implementeren van een strategie, met name effecten die tot nieuwe voorschriften inzake administratieve verwerking zullen leiden.

A65. Gewoonlijk identificeert het management bedrijfsrisico's en ontwikkelt het benaderingen om hier op in te spelen. Zo'n risico-inschattingsproces maakt deel uit van het interne beheersingssysteem van de entiteit en wordt in paragraaf 22 en de paragrafen A109-A113 besproken.

Overwegingen specifiek voor entiteiten in de publieke sector

A66. Entiteiten die actief zijn in de publieke sector, kunnen op verschillende manieren waarde creëren en leveren ten opzichte van degenen die rijkdom creëren voor eigenaren, maar zullen nog steeds een 'bedrijfsmodel' hebben met een specifieke doelstelling. Aangelegenheden waarin auditors in de publieke sector inzicht kunnen verwerven die relevant zijn voor het bedrijfsmodel van de entiteit, omvatten:

- kennis van relevante overheidsactiviteiten, inclusief gerelateerde programma's;
- programmadoelstellingen en -strategieën, inclusief elementen van overheidsbeleidslijnen.

A67. Voor de controles van entiteiten in de publieke sector kunnen "managementdoelstellingen" worden beïnvloed door vereisten om publieke verantwoording aan te tonen en kunnen zij doelstellingen omvatten die hun oorsprong hebben in wet- en regelgeving of andere van kracht zijnde voorschriften.

Sectorgebonden factoren, regelgevingsfactoren en andere externe factoren (Zie par. 19(a)(ii))

Sectorgebonden factoren

A68. Relevante sectorgebonden factoren zijn omstandigheden in de sector zoals de concurrentieomgeving, de relaties met leverancier en cliënten en technologische ontwikkelingen. Aangelegenheden die de auditor kan overwegen omvatten:

- de markt en concurrentie, inclusief vraag, capaciteit en prijsconcurrentie;
- cyclische of seizoensgebonden activiteit;
- technologie met betrekking tot de producten van de entiteit;
- de energievoorziening en kosten.

A69. De sector waarin de entiteit actief is, kan aanleiding geven tot specifieke risico's op een afwijking van materieel belang die voortkomt uit de aard van de activiteit of de mate van regulering.

Voorbeeld:
In de bouwsector kunnen langetermijncontracten significante schattingen van opbrengsten en kosten omvatten die aanleiding geven tot risico's op een afwijking van materieel belang. In dergelijke gevallen is het belangrijk dat het opdrachtteam bestaat uit leden met de passende competentie en capaciteiten.[33]

Regelgevingsfactoren

A70. Het regelgevingskader behoort tot de relevante regelgevingsfactoren. Het regelgevingskader omvat onder meer het van toepassing zijnde stelsel inzake financiële verslaggeving en de juridische en politieke omgeving en eventuele wijzigingen daarvan. Aangelegenheden die de auditor kan overwegen, omvatten:

- het regelgevingskader voor een gereguleerde sector, bijvoorbeeld prudentiële vereisten, inclusief vereisten voor toelichtingen;
- wet- en regelgeving die de activiteiten van de entiteit, significant beïnvloedt bijvoorbeeld op het gebied van arbeid;
- fiscale wet- en regelgeving;

[33] ISA 220 (herzien), paragrafen 25-28.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

- overheidsbeleidslijnen die op dat moment van invloed zijn op de uitvoering van de activiteiten van de entiteit, zoals het monetaire beleid, het begrotingsbeleid, financiële stimuleringsmaatregelen (bijvoorbeeld programma's voor overheidssteun) en beleidslijnen inzake douanerechten of handelsbelemmeringen;
- milieueisen die van invloed zijn op de activiteiten van de sector en de entiteit.

A71. ISA 250 (herzien) bevat enkele specifieke vereisten met betrekking tot het wet- en regelgevingskader dat van toepassing is op de entiteit en de branche of sector waarin de entiteit actief is.[34]

Overwegingen specifiek voor entiteiten in de publieke sector

A72. Voor de controles van entiteiten in de publieke sector kan er bepaalde wet-of regelgeving zijn die van invloed is op de activiteiten van de entiteit. Dergelijke elementen kunnen een essentiële overweging zijn bij het verwerven van inzicht de entiteit en haar omgeving.

Andere externe factoren

A73. Andere externe factoren die van invloed zijn op de entiteit en die de auditor kan overwegen, omvatten onder meer de algemene economische omstandigheden, de rentevoeten, de beschikbaarheid van financiering, de inflatie of de revaluatie van een munteenheid.

Door het management gebruikte maatstaven om de financiële prestaties van de entiteit in te schatten (Zie par. 19(a)(iii))

Waarom de auditor inzicht verwerft in de door het management gebruikte maatstaven

A74. Inzicht in de maatstaven van de entiteit helpt de auditor bij het overwegen of dergelijke maatstaven, extern of intern gebruikt, druk leggen op de entiteit om prestatiedoelen te bereiken. Deze druk kan het management motiveren om acties te ondernemen die de vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of fraude vergroten (bijv. om de bedrijfsprestaties te verbeteren of de financiële overzichten opzettelijk verkeerd weer te geven) (zie ISA 240 voor vereisten en leidraden met betrekking tot de risico's op fraude).

A75. Maatstaven kunnen de auditor ook wijzen op de waarschijnlijkheid van risico's op een afwijking van materieel belang van daarmee verband houdende informatie in de financiële overzichten. Prestatiemaatstaven kunnen bijvoorbeeld aangeven dat de entiteit een ongewoon snelle groei of winstgevendheid heeft in vergelijking met andere entiteiten in dezelfde sector.

Maatstaven die door het management worden gebruikt

A76. Het management en anderen meten en beoordelen gewoonlijk de aangelegenheden die zij belangrijk achten. Uit verzoeken om inlichtingen bij het management kan blijken dat het management zich baseert op bepaalde belangrijke indicatoren, openbaar beschikbaar of niet, voor het evalueren van financiële prestaties en het nemen van actie. In dergelijke gevallen kan de auditor relevante prestatiemaatstaven identificeren, intern of extern, door de informatie die de entiteit gebruikt om haar activiteiten te beheren, te overwegen. Als een dergelijk verzoek om inlichtingen duidt op een afwezigheid van prestatiemeting of beoordeling kan er een verhoogd risico zijn dat afwijkingen niet worden gedetecteerd en gecorrigeerd.

A77. Belangrijke indicatoren die worden gebruikt voor het evalueren van financiële prestaties kunnen omvatten:

- belangrijke (financiële en niet-financiële) prestatie-indicatoren en kernratio's, trends en bedrijfsstatistieken;

[34] ISA 250 (herzien), paragraaf 13.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

- vergelijkingen van financiële prestaties tussen verslagperiodes;
- budgetten, prognoses, verschillenanalyses, gesegmenteerde informatie en prestatieverslagen op divisie-, afdelings- of ander niveau;
- maatstaven voor de personeelsprestaties en beleidslijnen inzake op stimulansen gebaseerde beloningen;
- vergelijkingen van de prestaties van een entiteit met die van concurrenten.

Schaalbaarheid (Zie par. 19(a)(iii))

A78. De werkzaamheden die worden ondernomen om inzicht te verwerven in de maatstaven van de entiteit, kunnen variëren, afhankelijk van de grootte of complexiteit van de entiteit, evenals de betrokkenheid van eigenaren of de met governance belaste personen in het management van de entiteit.

Voorbeelden:

- Voor sommige minder complexe entiteiten kunnen de voorwaarden van de bankleningen van de entiteit (d.w.z. bankconvenanten) worden gekoppeld aan specifieke prestatiemaatstaven met betrekking tot de prestaties van de entiteit of de financiële positie (bijvoorbeeld een maximaal werkkapitaalbedrag). Het inzicht van de auditor in de prestatiemaatstaven die de bank gebruikt, kan helpen bij het identificeren van gebieden waar een hogere vatbaarheid is voor het risico op een afwijking van materieel belang.
- Voor sommige entiteiten waarvan de aard en omstandigheden complexer zijn, zoals degenen die actief zijn in de verzekerings- of banksector, kunnen prestaties of financiële positie gemeten worden aan wettelijke vereisten (bijv. wettelijke ratio-vereisten zoals kapitaaltoereikendheid en liquiditeitseisen). Het inzicht van de auditor in deze prestatiemaatstaven kan helpen bij het identificeren van gebieden met een hogere vatbaarheid voor het risico op een afwijking van materieel belang.

Andere overwegingen

A79. Externe partijen kunnen ook de financiële prestaties van de entiteit beoordelen en analyseren, met name voor entiteiten waar financiële informatie openbaar is. De auditor kan ook openbaar beschikbare informatie beschouwen om de hem te helpen beter inzicht te verwerven in de activiteiten of tegenstrijdige informatie te identificeren zoals informatie van:

- analisten of kredietbeoordelaars;
- nieuws en andere media, inclusief sociale media;
- belastingautoriteiten;
- regelgevers of toezichthouders;
- vakbonden;
- financiers.

Dergelijke financiële informatie kan vaak worden verkregen van de gecontroleerde entiteit.

A80. Het meten en beoordelen van financiële prestaties is niet hetzelfde als het monitoren van het systeem van interne beheersing (besproken als onderdeel van het systeem van interne beheersing in paragrafen A114-A122), hoewel hun doelen elkaar kunnen overlappen:

- de meting en beoordeling van prestaties is gericht op de vraag of bedrijfsprestaties voldoen aan de doelstellingen van het management (of van derden);
- het monitoren van het systeem van interne beheersing heeft daarentegen betrekking op het monitoren van de effectiviteit van interne beheersingsmaatregelen, inclusief degenen met betrekking tot de meting en beoordeling van de financiële prestatie door het management.

In sommige gevallen bieden prestatie-indicatoren echter ook informatie die het management in staat stelt om tekortkomingen in de interne beheersing te identificeren.

Overwegingen specifiek voor entiteiten in de publieke sector

A81. Naast het overwegen van relevante maatstaven die door een entiteit in de publieke sector worden gebruikt om de financiële prestaties van de entiteit in te schatten, kunnen auditors van entiteiten in de publieke sector ook niet-financiële informatie overwegen zoals het behalen van resultaten van algemeen nut (bijvoorbeeld het aantal mensen dat wordt bijgestaan door een specifiek programma).

Het van toepassing zijnde stelsel inzake financiële verslaggeving (Zie par. 19(b))

Inzicht in het van toepassing zijnde stelsel inzake financiële verslaggeving en de grondslagen voor financiële verslaggeving van de entiteit

A82. Aangelegenheden die de auditor kan overwegen bij het verkrijgen van inzicht in het van toepassing zijnde stelsel voor financiële verslaggeving van de entiteit en hoe dit van toepassing is in de context van de aard en omstandigheden van de entiteit en haar omgeving omvatten:

- de financiële verslaggevingspraktijken van de entiteit in termen van het van toepassing zijnde stelsel inzake financiële verslaggeving, zoals:
  - verslaggevingsprincipes en sectorspecifieke praktijken, inclusief sectorspecifieke significante transactiestromen, rekeningsaldi en daarmee verband houdende toelichtingen in de financiële overzichten (bijvoorbeeld leningen en investeringen bij banken, of onderzoek en ontwikkeling bij farmaceutische bedrijven);
  - opbrengstverantwoording;
  - administratieve verwerking van financiële instrumenten, inclusief gerelateerde kredietverliezen;
  - activa, passiva en transacties in vreemde valuta;
  - administratieve verwerking van ongebruikelijke of complexe transacties, waaronder transacties in controversiële of nieuwe gebieden (bijvoorbeeld rekening houden met crypto valuta);
- inzicht in de keuze en toepassing van de grondslagen voor financiële verslaggeving door de entiteit, inclusief eventuele wijzigingen daarin, evenals de redenen daarvoor, kan aangelegenheden omvatten zoals:
  - de methoden die de entiteit gebruikt om significante en ongebruikelijke transacties te herkennen, te waarderen, te presenteren en toe te lichten;
  - het effect van significante grondslagen voor financiële verslaggeving in controversiële of nieuwe gebieden waarvoor er een gebrek is aan gezaghebbende leidraden of consensus;
  - wijzigingen in de omgeving, zoals wijzigingen in het van toepassing zijnde stelsel inzake financiële verslaggeving of belastinghervormingen die een wijziging in de grondslagen voor financiële verslaggeving van de entiteit noodzakelijk maken;
  - ISA's inzake financiële verslaggeving en wet- en regelgeving die nieuw zijn voor de entiteit en wanneer en hoe de entiteit dergelijke vereisten zal toepassen of naleven.

A83. Het verwerven van inzicht in de entiteit en haar omgeving kan de auditor helpen bij het overwegen waar wijzigingen in de financiële verslaggeving van de entiteit (bijvoorbeeld vanuit voorgaande verslagperioden) kunnen worden verwacht.

Voorbeeld:
Als de entiteit gedurende de verslagperiode een significante fusie of overname heeft gehad, zou de auditor waarschijnlijk veranderingen in transactiestromen, rekeningsaldi en daarmee verband houdende toelichtingen met betrekking tot die fusie of overname verwachten. Aan de andere kant, als er geen significante wijzigingen in het stelsel voor financiële verslaggeving waren gedurende de

verslagperiode, kan het inzicht van de auditor helpen bevestigen dat het inzicht verkregen in de voorgaande verslagperiode van toepassing blijft.

Overwegingen specifiek voor entiteiten in de publieke sector

A84. Het van toepassing zijnde stelsel voor financiële verslaggeving in een entiteit in de publieke sector wordt bepaald door de wet- en regelgevingskaders die relevant zijn voor elke jurisdictie of binnen elk geografisch gebied. Aangelegenheden die overwogen kunnen worden bij de toepassing door de entiteit van het van toepassing zijnde stelsel inzake financiële verslaggeving en hoe het van toepassing is in de context van de aard en omstandigheden van de entiteit en haar omgeving, omvatten of de entiteit financiële verslaggeving volledig op basis van toerekening of op kasbasis toepast in overeenstemming met de *International Public Sector Accounting Standards*, of een hybride vorm.

Hoe inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden (Zie par. 19(c))

Bijlage 2 geeft voorbeelden van gebeurtenissen en omstandigheden die aanleiding kunnen geven voor het bestaan van risico's op een afwijking van materieel belang, ingedeeld naar inherente risicofactor.

Waarom de auditor inzicht verwerft in inherente risicofactoren bij het verwerven van inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving

A85. Inzicht in de entiteit en haar omgeving, en het van toepassing zijnde stelsel inzake financiële verslaggeving, helpt de auditor bij het identificeren van gebeurtenissen of omstandigheden, waarvan de kenmerken de vatbaarheid van beweringen over transactiestromen, rekeningsaldi of toelichtingen voor afwijkingen beïnvloeden. Deze kenmerken zijn inherente risicofactoren. Inherente risicofactoren kunnen de vatbaarheid van beweringen voor afwijkingen beïnvloeden door de waarschijnlijkheid van het voorkomen of de orde van grootte van de afwijking als deze zich zou voordoen te beïnvloeden. Inzicht in hoe inherent risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden, kan de auditor helpen met een voorlopig inzicht in de waarschijnlijkheid of omvang van afwijkingen, dat de auditor helpt bij het identificeren van risico's op een afwijking van materieel belang op het niveau van beweringen in overeenstemming met paragraaf 28(b). Inzicht in de mate waarin inherente risicofactoren de vatbaarheid van beweringen voor afwijkingen beïnvloeden, helpt de auditor ook bij het inschatten van de waarschijnlijkheid en de orde van grootte van een mogelijke afwijking bij het inschatten van het inherente risico in overeenstemming met paragraaf 31(a). Overeenkomstig, kan inzicht in de inherente risicofactoren de auditor ook helpen bij het opzetten en verder uitvoeren van controlewerkzaamheden in overeenstemming met ISA 330.

A86. De identificatie door de auditor van risico's op een afwijking van materieel belang op het niveau van beweringen en de inschatting van inherent risico kan ook worden beïnvloed door controle-informatie die de auditor heeft verkregen bij het uitvoeren van andere risico-inschattingswerkzaamheden, verdere controlewerkzaamheden of bij het voldoen aan andere vereisten in de ISA's (zie paragrafen A95, A103, A111, A121, A124 en A151).

Het effect van inherente risicofactoren op een transactiestroom, rekeningsaldo of toelichting

A87. De mate van vatbaarheid voor een afwijking van een transactiestroom, rekeningsaldo of toelichting die voortkomt uit complexiteit of subjectiviteit hangt vaak nauw samen met de mate waaraan deze is onderworpen aan wijzigingen of onzekerheid.

Voorbeeld:
Als de entiteit een schatting heeft die is gebaseerd op veronderstellingen, waarvan de keuze onderworpen is aan significante oordeelsvorming, zal de waardering van de schatting waarschijnlijk worden beïnvloed door zowel subjectiviteit als onzekerheid.

A88. Hoe groter de mate waarin een transactiestroom, rekeningsaldo of toelichting vatbaar is voor een afwijking als gevolg van complexiteit of subjectiviteit, des te groter is de noodzaak voor de auditor om een professioneel-kritische instelling toe te passen. Wanneer een transactiestroom, rekeningsaldo of toelichting vatbaar is voor afwijkingen vanwege complexiteit, subjectiviteit, wijzigingen of onzekerheid, kunnen deze inherente risicofactoren mogelijkheden creëren voor tendentie bij het management, hetzij onopzettelijk of opzettelijk, en de vatbaarheid voor een afwijking als gevolg van tendentie bij het management beïnvloeden. De identificatie door de auditor van risico's op een afwijking van materieel belang en een inschatting van het inherente risico op het niveau van beweringen worden ook beïnvloed door de onderlinge relaties tussen inherente risicofactoren.

A89. Gebeurtenissen of omstandigheden die van invloed kunnen zijn op de vatbaarheid voor afwijkingen als gevolg van tendentie bij het management, kunnen ook van invloed zijn op de vatbaarheid voor afwijkingen als gevolg van andere frauderisicofactoren. Dienovereenkomstig kan dit relevante informatie zijn om te gebruiken in overeenstemming met paragraaf 24 van ISA 240, die van de auditor vereist om te evalueren of de informatie verkregen uit de andere risico-inschattingswerkzaamheden en daarmee verband houdende activiteiten erop duiden dat een of meer frauderisicofactoren aanwezig zijn.

Het verwerven van inzicht in het interne beheersingssysteem van de entiteit (Zie par. 21-27)

Bijlage 3 beschrijft verder de aard van het systeem van interne beheersing van de entiteit en inherente beperkingen van interne beheersing. Bijlage 3 geeft ook een nadere uitleg van de componenten van een systeem van interne beheersing voor de doelstellingen van de ISA's.

A90. Het inzicht van de auditor in het interne beheersingssysteem van de entiteit wordt verworven door risico inschattingswerkzaamheden die worden uitgevoerd om inzicht te verwerven in alle componenten van het systeem van interne beheersing zoals beschreven in de paragrafen 21-27 en deze te evalueren.

A91. Voor het doel van deze ISA, hoeven de componenten van het interne beheersingssysteem van de entiteit niet noodzakelijkerwijs te weerspiegelen hoe een entiteit haar systeem van interne beheersing opzet, implementeert en onderhoudt, of hoe zij een specifieke component kan classificeren. Entiteiten kunnen verschillende terminologie of stelsels gebruiken om de verschillende aspecten van het systeem van interne beheersing te beschrijven. Voor de doelstelling van een controle kunnen auditors ook andere terminologie of stelsels gebruiken, mits alle componenten die in deze ISA worden beschreven in aanmerking worden genomen.

Schaalbaarheid

A92. De manier waarop het interne beheersingssysteem van de entiteit is ontworpen, geïmplementeerd en onderhouden varieert met de grootte en complexiteit van een entiteit. Minder complexe entiteiten kunnen bijvoorbeeld minder gestructureerde of eenvoudigere interne beheersingsmaatregelen (d.w.z. beleidslijnen en procedures) gebruiken om hun doelstellingen te bereiken.

Overwegingen specifiek voor entiteiten in de publieke sector

A93. Auditors van entiteiten in de publieke sector hebben vaak aanvullende verplichtingen met betrekking tot interne beheersing, bijvoorbeeld om te rapporteren over de naleving van een vastgestelde gedragscode of om te rapporteren over uitgaven ten opzichte van het budget. Auditors van entiteiten in de publieke sector kunnen ook verantwoordelijkheden hebben om te rapporteren over naleving van wet- en regelgeving of andere van kracht zijnde voorschriften. Als gevolg hiervan, kunnen hun overwegingen over het systeem van interne beheersing breder en gedetailleerder zijn.

Informatietechnologie in de componenten van het interne beheersingssysteem van de entiteit

Bijlage 5 biedt verdere leidraden voor het verwerven van inzicht in het gebruik van IT door de entiteit in de componenten van het systeem van interne beheersing.

A94. De algehele doelstelling en reikwijdte van een controle verschilt niet bij een entiteit die hoofdzakelijk actief is in een handmatige omgeving, een volledig geautomatiseerde omgeving of een omgeving met een combinatie van handmatige en geautomatiseerde elementen (d.w.z. handmatige en geautomatiseerde interne beheersingsmaatregelen en andere middelen die worden gebruikt in het interne beheersingssysteem van de entiteit).

Inzicht in de aard van de componenten van het interne beheersingssysteem van de entiteit

A95. Bij het evalueren van de effectiviteit van de opzet van interne beheersingsmaatregelen en of deze zijn geïmplementeerd (zie paragrafen A175-A181), verschaft het inzicht van de auditor in elk van de componenten van het systeem van interne beheersing van de entiteit een voorlopig inzicht in hoe de entiteit bedrijfsrisico's identificeert en hoe het daarop inspeelt. Het kan ook de identificatie en inschatting door de auditor van de risico's op een afwijking van materieel belang op verschillende manieren beïnvloeden (zie paragraaf A86). Dit helpt de auditor bij het opzetten en uitvoeren van verdere controlewerkzaamheden, inclusief eventuele plannen om de effectieve werking van interne beheersingsmaatregelen te toetsen. Bijvoorbeeld:

- Het inzicht van de auditor in de interne beheersingsomgeving van de entiteit, het risico-inschattingsproces van de entiteit, en het proces van de entiteit om componenten van interne beheersingsmaatregelen te monitoren, heeft waarschijnlijk meer invloed op de identificatie en inschatting van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten.
- Het inzicht van de auditor in het informatiesysteem en de communicatie van de entiteit, en de component "interne beheersingsactiviteiten" van de entiteit heeft waarschijnlijk meer invloed op de identificatie en inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen.

Interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheersing te monitoren (Zie par. 21-24)

A96. De interne beheersingsmaatregelen in de interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheersing te monitoren, zijn voornamelijk indirecte interne beheersingsmaatregelen (d.w.z. interne beheersingsmaatregelen die niet voldoende nauwkeurig zijn om afwijkingen op het niveau van beweringen te voorkomen, detecteren of te corrigeren, maar die andere interne beheersingsmaatregelen ondersteunen en daarom een indirect effect kunnen hebben op de waarschijnlijkheid dat een afwijking tijdig gedetecteerd of voorkomen wordt). Sommige interne beheersingsmaatregelen binnen deze componenten kunnen echter ook directe interne beheersingsmaatregelen zijn.

Waarom van de auditor vereist wordt inzicht te verwerven in de interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheersing te monitoren

A97. De interne beheersingsomgeving biedt een algemeen fundament voor de werking van de andere componenten van het systeem van interne beheersing. De interne beheersingsomgeving voorkomt, detecteert en corrigeert niet rechtstreeks afwijkingen. Het kan echter de effectiviteit van interne beheersingsmaatregelen in de andere componenten van het systeem van interne beheersing beïnvloeden. Evenzo zijn het risico-inschattingsproces van de entiteit en haar proces voor het monitoren van het systeem van interne beheersing ontworpen om op een manier te werken die ook het hele systeem van interne beheersing ondersteunt.

A98. Omdat deze componenten fundamenteel zijn voor het interne beheersingssysteem van de entiteit, kunnen tekortkomingen in hun werking gevolgen met een diepgaande invloed hebben voor het opstellen van de financiële overzichten. Daarom hebben het inzicht en de inschattingen van de auditor van deze componenten invloed op de identificatie en inschatting door de auditor van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en kan dit ook van invloed zijn op de identificatie en inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen. Risico's op een afwijking van materieel belang op het niveau van de financiële overzichten beïnvloeden de opzet van algehele manieren van inspelen door de auditor inclusief, zoals uitgelegd in ISA 330, een invloed op de aard, timing en omvang van de verdere werkzaamheden van de auditor.[35]

Inzicht verwerven in de interne beheersingsomgeving (Zie par. 21)

Schaalbaarheid

A99. De aard van de interne beheersingsomgeving in een minder complexe entiteit zal waarschijnlijk verschillen van de interne beheersingsomgeving in een meer complexe entiteit. Zo is het bijvoorbeeld mogelijk dat zich onder de met governance belaste personen in minder complexe entiteiten geen onafhankelijk of extern lid bevindt, en dat de governancefunctie direct door de eigenaar-bestuurder wordt waargenomen als er geen andere eigenaren zijn. Dienovereenkomstig zijn sommige overwegingen over de interne beheersingsomgeving van de entiteit mogelijk minder relevant of niet van toepassing.

A100. Bovendien is het mogelijk dat controle-informatie over elementen van de interne beheersingsomgeving in minder complexe entiteiten niet beschikbaar is in documentvorm, met name waar communicatie tussen management en ander personeel informeel is, maar de informatie kan nog steeds relevant en betrouwbaar zijn in de omstandigheden.

Voorbeelden:
- De organisatiestructuur in een minder complexe entiteit zal waarschijnlijk eenvoudiger zijn en kan een klein aantal werknemers dat betrokken is bij functies in verband met financiële verslaggeving omvatten.
- Als de rol van governance rechtstreeks door de eigenaar-bestuurder wordt ondernomen, kan de auditor bepalen dat de onafhankelijkheid van de met governance belaste personen niet relevant is.
- Minder complexe entiteiten hebben misschien geen schriftelijke gedragscode, maar ontwikkelen in plaats daarvan een cultuur die het belang van integriteit en ethisch gedrag benadrukt door mondelinge communicatie en door voorbeeldgedrag van het management. Bijgevolg zijn de houding, het bewustzijn en handelingen van het management of de eigenaar-bestuurder van bijzonder belang voor het inzicht van de auditor in de interne beheersingsomgeving van een minder complexe entiteit.

Inzicht in de interne beheersingsomgeving (Zie par. 21(a))

A101. Controle-informatie voor het inzicht van de auditor in de interne beheersingsomgeving kan worden verkregen via een combinatie van verzoeken om inlichtingen en andere risico-inschattingswerkzaamheden (d.w.z. bevestigende verzoeken om inlichtingen door waarneming of inspectie van documenten).

A102. Bij het overwegen van de mate waarin het management blijk geeft van toewijding aan integriteit en ethische waarden, kan de auditor inzicht verwerven door verzoeken om inlichtingen bij het management en werknemers en door informatie uit externe bronnen te overwegen, over:

- hoe het management zijn visie op bedrijfspraktijken en ethisch gedrag aan werknemers communiceert; en

[35] ISA 330, paragrafen A1-A3.

- inspectie van de schriftelijke gedragscode van het management en waarnemen of het management handelt op een manier die die code ondersteunt.

Evalueren van de interne beheersingsomgeving (Zie par. 21(b))

Waarom de auditor de interne beheersingsomgeving evalueert

A103. De evaluatie door de auditor:

- van hoe de entiteit gedrag vertoont dat consistent is met de toewijding van de entiteit aan integriteit en ethische waarden;
- of de interne beheersingsomgeving een geschikte basis biedt voor de andere componenten van het interne beheersingssysteem van de entiteit; en
- of geïdentificeerde tekortkomingen in de interne beheersing de andere componenten van het systeem van interne beheersing ondermijnen, helpt de auditor bij het identificeren van potentiële kwesties in de andere componenten van het interne beheersingssysteem. Dit komt omdat de interne beheersingsomgeving fundamenteel is voor de andere componenten van het interne beheersingssysteem van de entiteit. Deze evaluatie kan de auditor ook helpen bij het verwerven van inzicht in risico's waarmee de entiteit geconfronteerd wordt en daarom bij het identificeren en inschatten van de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het niveau van beweringen (Zie par. A86).

De evaluatie van de auditor van de interne beheersingsomgeving

A104. De evaluatie van de auditor van de interne beheersingsomgeving is gebaseerd op het inzicht verkregen in overeenstemming met paragraaf 21(a).

A105. Sommige entiteiten kunnen worden gedomineerd door een enkele persoon die veel zelf kan bepalen. De handelingen en houding van die persoon kunnen een diepgaande invloed hebben op de cultuur van de entiteit, die op haar beurt een diepgaande invloed kan hebben op de interne beheersingsomgeving. Een dergelijk effect kan positief of negatief zijn.

Voorbeeld:
Directe betrokkenheid door een enkele persoon kan cruciaal zijn om de entiteit in staat te stellen haar groei- en andere doelstellingen te realiseren en kan ook significant bijdragen aan een effectief systeem van interne beheersing. Anderzijds kan een dergelijke concentratie van kennis en autoriteit ook leiden tot een hogere vatbaarheid voor afwijkingen door het doorbreken van interne beheersmaatregelen door het management.

A106. De auditor kan overwegen hoe de verschillende elementen van de interne beheersingsomgeving kunnen worden beïnvloed door de filosofie en werkstijl van het senior management, rekening houdend met de betrokkenheid van onafhankelijke leden van de met governance belaste personen.

A107. Hoewel de interne beheersingsomgeving een geschikte basis kan vormen voor het systeem van interne beheersing en kan helpen het risico op fraude te verminderen, is een geschikte interne beheersingsomgeving niet noodzakelijk een effectief afschrikmiddel tegen fraude.

Voorbeeld:
Personeelsbeleidslijnen en procedures gericht op het aannemen van competent financieel, administratief, en IT-personeel kan het risico op fouten bij het verwerken en vastleggen van financiële informatie beperken. Dergelijk beleidslijnen en procedures kunnen echter niet de doorbreking van interne beheersingsmaatregelen door senior management beperken (bijvoorbeeld om winsten te overschatten).

A108. De evaluatie van de auditor van de interne beheersingsomgeving met betrekking tot het gebruik van IT door de entiteit kan aangelegenheden omvatten als:

- De vraag of governance over IT in verhouding staat tot de aard en complexiteit van de entiteit en haar bedrijfsactiviteiten mogelijk gemaakt door IT, inclusief de complexiteit of volwassenheid van het technologieplatform of architectuur van de entiteit en de mate waarin de entiteit afhankelijk is van IT-applicaties ter ondersteuning van haar financiële verslaggeving.
- De organisatiestructuur van het management met betrekking tot IT en de toegewezen middelen (bijvoorbeeld of de entiteit in een geschikte IT-omgeving en noodzakelijke verbeteringen heeft geïnvesteerd, of dat een voldoende aantal geschikte deskundige personen in dienst zijn, ook wanneer de entiteit commerciële software gebruikt (met geen of beperkte) modificaties)).

Verwerven van inzicht in het risico-inschattingsproces van de entiteit (Zie par. 22-23)

Inzicht in het risico-inschattingsproces van de entiteit (Zie par. 22(a))

A109. Zoals uitgelegd in paragraaf A62, geven niet alle bedrijfsrisico's aanleiding tot risico's op een afwijking van materieel belang. Bij het verwerven van inzicht in hoe het management en de met governance belaste personen bedrijfsrisico's hebben geïdentificeerd die relevant zijn voor het opstellen van de financiële overzichten en hebben besloten over handelingen om op deze risico's in te spelen, zijn aangelegenheden die de auditor kan overwegen onder meer hoe het management of, in voorkomend geval, de personen belast met governance:

- de doelstellingen van de entiteit met voldoende precisie en duidelijkheid heeft gespecificeerd om de identificatie en inschatting van de risico's met betrekking tot de doelstellingen mogelijk te maken;
- de risico's voor het bereiken van de doelstellingen van de entiteit heeft gespecificeerd en de risico's heeft geanalyseerd als basis voor het bepalen hoe de risico's moeten worden beheerd; en
- het potentieel voor fraude heeft beschouwd bij het overwegen van de risico's om de doelstellingen van de entiteit te bereiken.[36]

A110. De auditor kan de implicaties van dergelijke bedrijfsrisico's voor het opstellen van de financiële overzichten van de entiteit en andere aspecten van haar interne beheersingssysteem overwegen.

Evalueren van het risico-inschattingsproces van de entiteit (Zie par. 22(b))

Waarom de auditor evalueert of het risico-inschattingsproces van de entiteit geschikt is

A111. De evaluatie door de auditor van het risico-inschattingsproces van de entiteit kan de auditor helpen bij het verwerven van inzicht waar de entiteit risico's heeft geïdentificeerd die kunnen voorkomen en hoe de entiteit heeft ingespeeld op die risico's. De evaluatie van de auditor hoe de entiteit haar bedrijfsrisico's identificeert, inschat en erop inspeelt, helpt de auditor bij het inzicht of deze risico's als passend voor de aard en complexiteit van de entiteit zijn geïdentificeerd, ingeschat en erop ingespeeld. Deze evaluatie kan de auditor ook helpen bij het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het niveau van beweringen (Zie par. A86).

Evalueren of het risico-inschattingsproces van de entiteit geschikt is (Zie par. 22(b))

A112. De evaluatie door de auditor van de geschiktheid van het risico-inschattingsproces van de entiteit is gebaseerd op het inzicht verkregen in overeenstemming met paragraaf 22(a).

[36] ISA 240, paragraaf 19.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

Schaalbaarheid

A113. Of het risico-inschattingsproces van de entiteit geschikt is voor de omstandigheden gezien de aard en complexiteit van de entiteit is een kwestie van professionele oordeelsvorming door de auditor.

Voorbeeld:
In sommige minder complexe entiteiten, en met name door de eigenaar bestuurde entiteiten, kan een geschikte risico inschatting worden uitgevoerd door de directe betrokkenheid van het management of de eigenaar-bestuurder (de manager of eigenaar-bestuurder kan bijv. routinematig tijd besteden aan het monitoren van de activiteiten van concurrenten en andere ontwikkelingen in de markt om nieuwe bedrijfsrisico's te identificeren). De informatie van deze risico-inschatting in dit soort entiteiten is vaak niet formeel gedocumenteerd, maar uit de besprekingen die de auditor heeft met het management kan blijken dat het management in feite risico-inschattingswerkzaamheden uitvoert.

Het verwerven van inzicht in het proces van de entiteit om het interne beheersingssysteem van de entiteit te monitoren (Zie par. 24)

Schaalbaarheid

A114. In minder complexe entiteiten, en met name door de eigenaar bestuurde entiteiten, is het inzicht van de auditor van het proces van de entiteit om het systeem van interne beheersing te monitoren vaak gericht op hoe het management of de eigenaar-bestuurder direct betrokken is bij activiteiten, omdat er mogelijk geen andere monitoringactiviteiten zijn.

Voorbeeld:
Het management kan klachten van klanten ontvangen over onnauwkeurigheden in hun maandelijkse overzichten die de eigenaar-bestuurder alert maakt op kwesties met de timing wanneer klantbetalingen zijn opgenomen in de administratieve vastleggingen.

A115. Er zijn entiteiten die geen formeel proces voor het monitoren van het systeem van interne beheersing hebben. Bij deze entiteiten kan inzicht in het proces om het systeem van interne beheersing te monitoren inzicht in periodieke beoordelingen van management accounting informatie die is opgezet om bij te dragen aan hoe de entiteit afwijkingen voorkomt of detecteert, omvatten.

Inzicht in het proces van de entiteit om het systeem van interne beheersing te monitoren (Zie par. 24(a))

A116. Aangelegenheden die relevant kunnen zijn voor de auditor om te overwegen bij het verwerven van inzicht hoe de entiteit haar systeem van interne beheersing monitort, omvatten:

- de opzet van de monitoringactiviteiten, bijvoorbeeld of het periodieke of doorlopende monitoring is;
- de prestaties en frequentie van de monitoringactiviteiten;
- de evaluatie van de resultaten van de monitoringactiviteiten, op een tijdige basis, om te bepalen of de interne beheersingsmaatregelen effectief zijn geweest; en
- hoe vastgestelde tekortkomingen zijn behandeld door passende corrigerende maatregelen, inclusief tijdige communicatie van dergelijke tekortkomingen aan degenen die verantwoordelijk zijn voor het nemen van corrigerende maatregelen.

A117. De auditor kan ook overwegen hoe het proces van de entiteit om het systeem van interne beheersing te monitoren interne beheersingsmaatregelen voor informatieverwerking behandelt waarbij IT wordt gebruikt. Dit kan bijvoorbeeld omvatten:

- interne beheersingsmaatregelen om complexe IT-omgevingen te monitoren die:

  - de voortdurende effectieve opzet van interne beheersingsmaatregelen voor informatieverwerking evalueren en deze wijzigen, voor zover van toepassing, voor veranderingen in omstandigheden; of
  - de effectieve werking van interne beheersingsmaatregelen voor informatieverwerking evalueren;

- interne beheersingsmaatregelen die de toegangsrechten monitoren die zijn toegepast in geautomatiseerde interne beheersingsmaatregelen voor informatieverwerking die de functiescheiding afdwingen.
- interne beheersingsmaatregelen die monitoren hoe fouten of tekortkomingen in de interne beheersing met betrekking tot de automatisering van financiële verslaggeving worden geïdentificeerd en behandeld.

Inzicht in de interne auditfunctie van de entiteit (Zie par. 24(a)(ii))

Bijlage 4 bevat verdere overwegingen voor het verwerven van inzicht in de interne auditfunctie van de entiteit.

A118. De verzoeken om inlichtingen van de auditor bij geschikte personen binnen de interne auditfunctie helpen de auditor inzicht te verwerven in de aard van de verantwoordelijkheden van de interne auditfunctie. Als de auditor bepaalt dat de verantwoordelijkheden van de functie verband houden met de financiële verslaggeving van de entiteit, kan de auditor nader inzicht verwerven in de activiteiten die door de interne audit zijn uitgevoerd of zullen worden uitgevoerd door het auditplan van de interne auditfunctie voor de verslagperiode te beoordelen, voor zover dit bestaat, en dat plan te bespreken met de juiste personen binnen de functie. Dit inzicht, samen met de informatie die verkregen is uit verzoeken om inlichtingen van de auditor, kan ook informatie verschaffen die direct relevant is voor de identificatie en inschatting van de auditor van de risico's op een afwijking van materieel belang. Als de auditor op basis van het voorlopige inzicht van de auditor van de interne auditfunctie verwacht gebruik te maken van het werk van de interne auditfunctie om de aard of timing van controlewerkzaamheden te wijzigen of de omvang daarvan te verminderen, is ISA 610 (herzien 2013)[37] van toepassing.

Andere informatiebronnen die worden gebruikt in het proces van de entiteit om het systeem van interne beheersing te monitoren

Inzicht verwerven in de informatiebronnen (Zie par. 24(b))

A119. Tot de monitoringactiviteiten van het management kan behoren het gebruikmaken van informatie die uit communicatie met externe partijen is verkregen zoals klachten van klanten of opmerkingen van regelgevende instanties die kunnen duiden op problemen of die de aandacht vestigen op gebieden waarop verbeteringen nodig zijn.

Waarom van de auditor vereist wordt inzicht te verwerven in de informatiebronnen die worden gebruikt voor het monitoren van het systeem van interne beheersing van de entiteit

A120. Het inzicht van de auditor in de informatiebronnen die door de entiteit worden gebruikt bij het monitoren van het systeem van interne beheersing van de entiteit, inclusief of de gebruikte informatie relevant en betrouwbaar is, helpt de auditor bij het evalueren of het proces van de entiteit om het systeem van interne beheersing van de entiteit te monitoren, geschikt is. Als het management veronderstelt dat informatie die wordt gebruikt voor monitoring relevant en betrouwbaar is zonder een basis voor die veronderstelling te hebben, kunnen eventuele fouten in de informatie ertoe leiden dat het management verkeerde conclusies trekt uit zijn monitoringactiviteiten.

[37] ISA 610 (herzien 2013), *Gebruikmaken van het werk van interne auditors.*

Evalueren van het proces van de entiteit om het systeem van interne beheersing te monitoren (Zie par. 24(c))

Waarom de auditor evalueert of het proces van de entiteit om het systeem van interne beheersing te monitoren, geschikt is

A121. De evaluatie van de auditor over hoe de entiteit doorlopende en afzonderlijke evaluaties onderneemt voor het monitoren van de effectiviteit van interne beheersingsmaatregelen, helpt de auditor bij het verwerven van inzicht of de ander componenten van het interne beheersingssysteem van de entiteit aanwezig zijn en functioneren. Dit helpt daarom bij het verwerven van inzicht in de andere componenten van het interne beheersingssysteem van de entiteit. Deze evaluatie kan de auditor ook helpen bij het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en op het niveau van beweringen (Zie par. A86).

Evalueren of het proces van de entiteit om het systeem van interne beheersing te controleren, geschikt is (Zie par. 24(c))

A122. De evaluatie door de auditor van de geschiktheid van het proces van de entiteit om het systeem van interne beheersing te monitoren, is gebaseerd op het inzicht van de auditor in het proces van de entiteit om het systeem van interne beheersing te monitoren.

Informatiesysteem en communicatie en interne beheersingsactiviteiten (Zie par. 25-26)

A123. De componenten interne beheersingsmaatregelen in het "informatiesysteem en communicatie" en "interne beheersingsactiviteiten" zijn primair directe interne beheersingsmaatregelen (d.w.z. interne beheersingsmaatregelen die voldoende nauwkeurig zijn om afwijkingen op het niveau van beweringen te voorkomen, detecteren of corrigeren).

Waarom van de auditor vereist wordt inzicht te verwerven in het informatiesysteem en communicatie en interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"

A124. Van de auditor wordt vereist om inzicht te verwerven in het informatiesysteem en de communicatie van de entiteit omdat:

- inzicht in de beleidslijnen van de entiteit die de transactiestromen en andere aspecten van de informatieverwerkingsactiviteiten van de entiteit definiëren die relevant zijn voor het opstellen van de financiële overzichten, en
- evalueren of de component op passende wijze het opstellen van de financiële overzichten van de entiteit ondersteunt, de identificatie en inschatting van de auditor van risico's op een afwijking van materieel belang op het niveau van beweringen ondersteunt. Dit inzicht en deze evaluatie kunnen ook leiden tot de identificatie van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten, wanneer de resultaten van de werkzaamheden van de auditor niet consistent zijn met verwachtingen over het systeem van interne beheersing van de entiteit dat mogelijk was opgesteld op basis van informatie die verkregen is tijdens het proces voor aanvaarding of continuering van de opdracht (Zie par. A86).

A125. Van de auditor wordt vereist om specifieke interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten" te identificeren, de opzet te evalueren en te bepalen of de interne beheersingsmaatregelen zijn geïmplementeerd, aangezien dit de auditor helpt inzicht te verwerven in de aanpak van het management om in te spelen op bepaalde risico's. Dit biedt daarom een basis voor de opzet en de uitvoering van verdere controlewerkzaamheden die inspelen op deze risico's, zoals vereist door ISA 330. Hoe hoger op het spectrum van inherent risico een risico is ingeschat, hoe overtuigender de controle-informatie moet zijn. Zelfs wanneer de auditor niet van plan is om de effectieve werking van geïdentificeerde interne beheersingsmaatregelen te toetsen, kan het inzicht van de auditor nog steeds van invloed zijn op

de opzet van de aard, timing en omvang van gegevensgerichte controlewerkzaamheden die inspelen op de daarmee samenhangende risico's op een afwijking van materieel belang.

De iteratieve aard van het inzicht en de evaluatie van de auditor van het informatiesysteem en communicatie- en interne beheersingsactiviteiten

A126. Zoals uitgelegd in paragraaf A49, verwerft de auditor inzicht in de entiteit en haar omgeving en het van toepassing zijnde stelsel inzake financiële verslaggeving. Dit inzicht kan de auditor helpen bij het ontwikkelen van initiële verwachtingen over de transactiestromen, rekeningsaldi en toelichtingen die significante transactiestromen, rekeningsaldi en toelichtingen kunnen zijn. Bij het verwerven van inzicht in de component "informatie systeem en communicatie" in overeenstemming met paragraaf 25(a), kan de auditor deze initiële verwachtingen gebruiken om de mate van inzicht in de informatieverwerkingsactiviteiten van de entiteit die moet worden verkregen, te bepalen.

A127. Het inzicht van de auditor in het informatiesysteem omvat het verwerven van inzicht in de beleidslijnen die informatiestromen met betrekking tot de significante transactiestromen, rekeningsaldi en toelichtingen van de entiteit en andere gerelateerde aspecten van de informatieverwerkingsactiviteiten van de entiteit definiëren. Deze informatie, en de informatie verkregen uit de evaluatie van de auditor van het informatiesysteem, kan de verwachtingen van de auditor over de significante transactiestromen, rekeningsaldi en toelichtingen die aanvankelijk zijn geïdentificeerd, bevestigen of verder beïnvloeden (Zie par. A126).

A128. Om inzicht te verwerven in hoe informatie met betrekking tot significante transactiestromen, rekeningsaldi en toelichtingen in, door en uit het informatiesysteem van de entiteit stroomt, kan de auditor ook interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten" identificeren die moeten worden geïdentificeerd in overeenstemming met paragraaf 26(a). De identificatie en evaluatie van interne beheersingsmaatregelen door de auditor in de component "interne beheersingsactiviteiten" kan zich eerst richten op interne beheersingsmaatregelen op journaalboekingen en interne beheersingsmaatregelen waarvan de auditor van plan is om de effectieve werking te toetsen bij het opzetten van de aard, timing en omvang van gegevensgerichte werkzaamheden.

A129. De inschatting door de auditor van inherent risico kan ook het onderkennen van interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten" beïnvloeden. De identificatie van interne beheersingsmaatregelen door de auditor met betrekking tot significante risico's kan bijvoorbeeld alleen te onderkennen zijn wanneer de auditor het inherente risico op het niveau van beweringen heeft ingeschat in overeenstemming met paragraaf 31. Bovendien kunnen interne beheersingsmaatregelen die inspelen op risico's waarvoor de auditor heeft vastgesteld dat gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen, (in overeenstemming met paragraaf 33), ook pas te onderkennen zijn als de inschattingen van het inherente risico door de auditor zijn uitgevoerd.

A130. De identificatie en inschatting door de auditor van risico's op een afwijking van materieel belang op het niveau van beweringen wordt beïnvloed door zowel:

- inzicht van de auditor in de beleidslijnen van de entiteit voor haar informatieverwerkingsactiviteiten in de component "informatiesysteem- en communicatie", en
- identificatie en evaluatie van de auditor van interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten".

Inzicht verwerven in het informatiesysteem en de communicatie (Zie par. 25)

Bijlage 3, paragrafen 15-19, bevat verdere overwegingen met betrekking tot het informatiesysteem en communicatie.

Schaalbaarheid

A131. Het informatiesysteem en gerelateerde bedrijfsprocessen in minder complexe entiteiten zullen waarschijnlijk minder geavanceerd zijn dan in grotere entiteiten, en zal waarschijnlijk een minder complexe IT-omgeving met zich meebrengen; echter, de rol van het informatiesysteem is net zo belangrijk. Minder complexe entiteiten met een directe betrokkenheid van het management hebben mogelijk geen behoefte aan uitgebreide beschrijvingen van administratieve verwerkingsprocedures, ingewikkelde administratieve vastleggingen of uitgeschreven beleidslijnen. Inzicht in de relevante aspecten van het informatiesysteem van de entiteit kan daarom minder inspanning vergen bij een controle van een minder complexe entiteit en kan een groter aantal verzoeken om inlichtingen dan waarneming of inspectie van documentatie inhouden. De noodzaak om inzicht te verwerven blijft echter belangrijk om een basis te vormen voor de opzet van verdere controlewerkzaamheden in overeenstemming met ISA 330 en kan de auditor verder helpen bij het identificeren of inschatten van risico's op een afwijking van materieel belang (Zie par. A86).

Inzicht verwerven in het informatiesysteem (Zie par. 25(a))

A132. In het interne beheersingssysteem van de entiteit zijn aspecten opgenomen die betrekking hebben op de verslaggevingsdoelstellingen van de entiteit, inclusief de financiële verslaggevingsdoelstellingen, maar kunnen ook aspecten omvatten die betrekking hebben op de doelstellingen op het gebied van de activiteiten of de naleving van wet- en regelgeving, wanneer dergelijke aspecten relevant zijn voor financiële verslaggeving. Inzicht in hoe de entiteit transacties initieert en informatie vastlegt als onderdeel van het inzicht van de auditor in het informatiesysteem kan informatie omvatten over de systemen van de entiteit (haar beleidslijnen) die zijn opgezet om nalevings- en operationele doelstellingen te bereiken, omdat dergelijke informatie relevant is voor het opstellen van de financiële overzichten. Verder kunnen sommige entiteiten informatie systemen hebben die in hoge mate geïntegreerd zijn zodat interne beheersingsmaatregelen op een manier kunnen worden opgezet om tegelijkertijd financiële verslaggevings-, compliance- en operationele doelstellingen en combinaties daarvan te bereiken.

A133. Inzicht in het informatiesysteem van de entiteit omvat ook inzicht in de middelen die worden gebruikt bij de informatieverwerkingsactiviteiten van de entiteit. Informatie over de betrokken personele inzet die relevant kan zijn voor het verwerven van inzicht in risico's voor de integriteit van het informatiesysteem zijn onder meer:

- de competentie van de personen die het werk uitvoeren;
- of er voldoende middelen zijn; en
- of er sprake is van een passende functiescheiding.

A134. Aangelegenheden die de auditor kan overwegen bij het verwerven van inzicht in de beleidslijnen die de informatiestromen definiëren met betrekking tot de significante transactiestromen, rekeningsaldi en toelichtingen van de entiteit in de component "informatiesysteem en communicatie" omvatten de aard van:

(a) de gegevens of informatie met betrekking tot te verwerken transacties, andere gebeurtenissen en omstandigheden;
(b) de informatieverwerking om de integriteit van die gegevens of informatie te handhaven; en
(c) de informatieprocessen, personeel en andere middelen die bij het informatieverwerkingsproces worden gebruikt.

A135. Verwerven van inzicht in de bedrijfsprocessen van de entiteit, waaronder hoe transacties zijn ontstaan, helpt de auditor bij het verwerven van inzicht in het informatiesysteem van de entiteit op een manier die geschikt is voor de omstandigheden van de entiteit.

A136. Het inzicht van de auditor in het informatiesysteem kan op verschillende manieren worden verkregen en kan omvatten:

- verzoeken om inlichtingen bij relevant personeel over de procedures die worden gebruikt voor het initiëren, vastleggen, verwerken en rapporteren van transacties of over het financiële verslaggevingsproces van de entiteit;
- inspectie van beleidslijnen of proceshandboeken of andere documentatie van het informatiesysteem van de entiteit;
- waarneming van de uitvoering van de beleidslijnen of de procedures door het personeel van de entiteit; of
- transacties selecteren en traceren via het van toepassing zijnde proces in het informatiesysteem (d.w.z. een lijncontrole uitvoeren).

Geautomatiseerde hulpmiddelen en technieken

A137. De auditor kan ook geautomatiseerde technieken gebruiken om directe toegang tot of een digitale download te verkrijgen van de databases in het informatiesysteem van de entiteit die administratieve vastleggingen van transacties opslaan. Door geautomatiseerde hulpmiddelen of technieken op deze informatie toe te passen, kan de auditor het verkregen inzicht bevestigen over hoe transacties door het informatiesysteem stromen door journaalboekingen of andere digitale vastleggingen met betrekking tot een bepaalde transactie of een volledige populatie van transacties, te traceren van initiatie in de administratieve vastleggingen tot opname in het grootboek. Analyse van complete of grote sets transacties kan ook leiden tot het identificeren van variaties van de normale of verwachte verwerkingsprocedures voor deze transacties, die kunnen leiden tot de identificatie van risico's op een afwijking van materieel belang.

Informatie verkregen buiten het grootboek en subgrootboeken

A138. Financiële overzichten kunnen informatie bevatten die is verkregen buiten het grootboek en subgrootboeken. Voorbeelden van dergelijke informatie die de auditor kan overwegen omvatten:

- informatie verkregen uit leaseovereenkomsten die relevant zijn voor toelichtingen in de financiële overzichten;
- informatie toegelicht in de financiële overzichten die wordt geproduceerd door het risicomanagementsysteem van een entiteit;
- informatie over reële waarde die door deskundigen ingeschakeld door het management is geproduceerd en toegelicht in de financiële overzichten;
- informatie toegelicht in de financiële overzichten die is verkregen uit modellen of uit andere berekeningen die gebruikt zijn om schattingen te ontwikkelen die zijn opgenomen of toegelicht worden in de financiële overzichten, inclusief informatie met betrekking tot de onderliggende gegevens en veronderstellingen die gebruikt zijn in die modellen, zoals:
  - intern ontwikkelde veronderstellingen die de gebruiksduur van een actief kunnen beïnvloeden; of
  - gegevens zoals rentevoeten die worden beïnvloed door factoren waarop de entiteit geen invloed heeft.
- informatie toegelicht in de financiële overzichten over gevoeligheidsanalyses afgeleid van financiële modellen die aantoont dat het management alternatieve veronderstellingen heeft overwogen;
- informatie opgenomen of toegelicht in de financiële overzichten die is verkregen uit de belastingaangiften en vastleggingen van de entiteit;
- informatie toegelicht in de financiële overzichten die is verkregen uit analyses die zijn opgesteld om de beoordeling van het management van de mogelijkheid van de entiteit om haar continuïteit te handhaven te ondersteunen, zoals eventuele toelichtingen met betrekking tot gebeurtenissen of omstandigheden die zijn geïdentificeerd die gerede twijfel kunnen doen ontstaan over de mogelijkheid van de entiteit om continuïteit te handhaven.[38]

[38] ISA 570, paragrafen 19-20.

A139. Bepaalde bedragen of toelichtingen in de financiële overzichten van de entiteit (zoals toelichtingen over kredietrisico, liquiditeitsrisico en marktrisico) kunnen gebaseerd zijn op informatie verkregen uit het risicomanagementsysteem van de entiteit. De auditor hoeft echter geen inzicht te verwerven in alle aspecten van het risicomanagementsysteem, en past professionele oordeelsvorming toe bij het bepalen van het benodigde inzicht.

Het gebruik van informatietechnologie door de entiteit in het informatiesysteem

Waarom verwerft de auditor inzicht in de IT-omgeving die relevant is voor het informatiesysteem

A140. Het inzicht van de auditor in het informatiesysteem omvat de IT-omgeving die relevant is voor de transactiestromen en informatieverwerking in het informatiesysteem van de entiteit omdat de het gebruik van IT-applicaties door de entiteit of andere aspecten in de IT-omgeving aanleiding kan geven tot risico's van het gebruik van IT.

A141. Het inzicht in het bedrijfsmodel van de entiteit en hoe het gebruik van IT wordt geïntegreerd, kan ook nuttige context bieden voor de aard en omvang van IT die in het informatiesysteem wordt verwacht.

Inzicht in het gebruik van IT door de entiteit

A142. Het inzicht van de auditor in de IT-omgeving kan gericht zijn op het identificeren en verwerven van inzicht in de aard en aantal van de specifieke IT-applicaties en andere aspecten van de IT-omgeving die relevant zijn voor de stromen van transacties en informatieverwerking in het informatiesysteem. Veranderingen in de stroom van transacties of informatie binnen het informatiesysteem kunnen het gevolg zijn van programma wijzigingen in IT-applicaties of directe wijzigingen in gegevens in databases die betrokken zijn bij de verwerking of opslag van die transacties of informatie.

A143. De auditor kan de IT-applicaties en de ondersteunende IT-infrastructuur gelijktijdig identificeren met het inzicht van de auditor in hoe informatie met betrekking tot significante transactiestromen, rekening saldi en toelichtingen in, door en uit het informatiesysteem van de entiteit stromen.

Het verwerven van inzicht in de communicatie van de entiteit (Zie par. 25(b))

Schaalbaarheid

A144. In grotere, meer complexe entiteiten, kan informatie die de auditor kan overwegen bij het verwerven van inzicht in de communicatie van de entiteit afkomstig zijn van handboeken over beleidsprocedures en over financiële verslaggeving.

A145. In minder complexe entiteiten kan communicatie minder gestructureerd zijn (formele handboeken worden bijvoorbeeld niet gebruikt) vanwege minder verantwoordelijkheidsniveaus en een grotere zichtbaarheid en beschikbaarheid van het management. Ongeacht de grootte van de entiteit vergemakkelijken open communicatiekanalen de rapportage van uitzonderingen en het ernaar handelen.

Evalueren of de relevante aspecten van het informatiesysteem het opstellen van de financiële overzichten van de entiteit ondersteunen (Zie par. 25(c))

A146. De evaluatie door de auditor of het informatiesysteem en de communicatie van de entiteit de opstelling van de financiële overzichten op passende wijze ondersteunt, is gebaseerd op het inzicht verkregen in paragraaf 25(a)-(b).

Interne beheersingsactiviteiten (Zie par. 26)

Interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"

Bijlage 3, paragrafen 20 en 21 bevatten verdere overwegingen met betrekking tot interne beheersingsactiviteiten.

A147. De component "interne beheersingsactiviteiten" omvat interne beheersingsmaatregelen die zijn opgezet om te zorgen voor de juiste toepassing van beleidslijnen (die ook interne beheersingsmaatregelen zijn) in alle andere componenten van het interne beheersingssysteem van de entiteit en omvat zowel directe als indirecte interne beheersingsmaatregelen.

Voorbeeld:
De interne beheersingsmaatregelen die een entiteit heeft ingesteld om ervoor te zorgen dat haar personeel de jaarlijkse fysieke voorraad naar behoren opneemt en vastlegt houden rechtstreeks verband met de risico's op een afwijking van materieel belang die relevant zijn voor de beweringen "bestaan" en "volledigheid" voor het rekeningsaldo van de voorraad.

A148. De identificatie en evaluatie van interne beheersingsmaatregelen door de auditor in de component "interne beheersingsactiviteiten" is gericht op interne beheersingsmaatregelen voor informatieverwerking. Dit zijn interne beheersingsmaatregelen die worden toegepast tijdens de verwerking van informatie in het informatiesysteem van de entiteit die direct inspelen op risico's voor de integriteit van informatie (d.w.z. de volledigheid, nauwkeurigheid en geldigheid van transacties en andere informatie). Van de auditor wordt echter niet vereist om alle interne beheersingsmaatregelen voor informatieverwerking met betrekking tot de beleidslijnen van de entiteit die de transactiestromen en andere aspecten van de informatieverwerkingsactiviteiten van de entiteit definiëren voor de significante transactiestromen, rekeningsaldi en toelichtingen te identificeren en te evalueren.

A149. Er kunnen ook directe interne beheersingsmaatregelen zijn die bestaan in de interne beheersingsomgeving, het risico-inschattingsproces van de entiteit of het proces van de entiteit om het systeem van interne beheersing te monitoren, die kunnen worden geïdentificeerd in overeenstemming met paragraaf 26. Hoe indirecter de relatie tussen interne beheersingsmaatregelen die andere interne beheersingsmaatregelen ondersteunen en de interne beheersingsmaatregel die worden overwogen echter is, hoe minder effectief die interne beheersingsmaatregel kan zijn bij het voorkomen, of detecteren en corrigeren van gerelateerde afwijkingen.

Voorbeeld:
Gewoonlijk is een beoordeling door een verkoopmanager van een samenvatting van de verkoopactiviteit voor specifieke winkels per regio alleen indirect gerelateerd aan de risico's op een afwijking van materieel belang die relevant is voor de bewering van de volledigheid van verkoopopbrengsten. Dienovereenkomstig kan het minder effectief zijn om in te spelen op die risico's dan interne beheersingsmaatregelen die directer daaraan zijn gerelateerd, zoals de aansluiting van vervoersdocumenten met factuurdocumenten.

A150. Paragraaf 26 vereist ook dat de auditor *general IT controls* voor IT-applicaties en andere aspecten van de IT-omgeving identificeert en evalueert, waarvan de auditor heeft vastgesteld dat deze onderhevig zijn aan risico's die voortkomen het gebruik van IT, omdat *general IT controls* de blijvende effectieve werking van interne beheersingsmaatregelen voor informatieverwerking ondersteunen. Een *general IT-control* alleen is meestal niet voldoende om in te spelen op risico op een afwijking van materieel belang op het niveau van beweringen.

A151. De interne beheersingsmaatregelen waarvan de auditor de opzet moet identificeren en evalueren en de implementatie daarvan moet bepalen in overeenstemming met paragraaf 26, zijn:

- interne beheersingsmaatregelen waarvan de auditor van plan is om de effectieve werking te toetsen voor het bepalen van de aard, timing en omvang van gegevensgerichte werkzaamheden. De evaluatie van dergelijke interne beheersingsmaatregelen vormt de

basis voor de opzet van de auditor van het toetsen van interne beheersingsmaatregelen in overeenstemming met ISA 330. Deze interne beheersingsmaatregelen omvatten ook interne beheersingsmaatregelen die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen;

- interne beheersingsmaatregelen die inspelen op significante risico's en interne beheersingsmaatregelen over journaalboekingen. De identificatie en evaluatie van dergelijke interne beheersingsmaatregelen door de auditor kunnen ook van invloed zijn op het inzicht van de auditor in de risico's op een afwijking van materieel belang, inclusief de identificatie van aanvullende risico's op een afwijking van materieel belang (zie par. A95). Dit inzicht biedt ook de basis voor de opzet van de auditor van de aard, timing en omvang van gegevensgerichte controlewerkzaamheden die inspelen op de gerelateerde ingeschatte risico's op een afwijking van materieel belang;
- andere interne beheersingsmaatregelen die de auditor overweegt zijn geschikt om hem in staat te stellen de doelstellingen van paragraaf 13 met betrekking tot risico's op het niveau van beweringen te bereiken, gebaseerd op de professionele oordeelsvorming van de auditor.

A152. Interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"" moeten worden geïdentificeerd wanneer dergelijke interne beheersingsmaatregelen voldoen aan een of meer van de criteria in paragraaf 26(a). Wanneer echter meerdere interne beheersingsmaatregelen dezelfde doelstelling bereiken, is het niet nodig om elk van de interne beheersingsmaatregelen met betrekking tot een dergelijke doelstelling te identificeren.

Typen interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"" (Zie par. 26)

A153. Voorbeelden van interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"" zijn autorisaties en goedkeuringen, aansluitingen, verificaties (zoals bewerkings- en validatie controles of geautomatiseerde berekeningen), functiescheiding en fysieke of logische interne beheersingsmaatregelen, inclusief die voor de bescherming van activa.

A154. Interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"" kunnen ook interne beheersingsmaatregelen omvatten die zijn vastgesteld door het management die inspelen op risico's op een afwijking van materieel belang in verband met toelichtingen die niet in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving zijn opgesteld. Dergelijke interne beheersingsmaatregelen kunnen betrekking hebben op informatie die is opgenomen in de financiële overzichten die is verkregen buiten het grootboek en subgrootboeken.

A155. Ongeacht of interne beheersingsmaatregelen zich binnen de IT-omgeving of in handmatige systemen bevinden, kunnen interne beheersingsmaatregelen verschillende doelstellingen hebben en kunnen ze worden toegepast op verschillende organisatorische en functionele niveaus.

Schaalbaarheid (Zie par. 26)

A156. Interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten" voor minder complexe entiteiten zijn waarschijnlijk vergelijkbaar met die in grotere entiteiten, maar de formaliteit waarmee ze werken kan variëren. Verder kunnen in minder complexe entiteiten meer interne beheersingsmaatregelen direct door het management worden toegepast.

Voorbeeld:
De exclusieve bevoegdheid van het management om klanten krediet te verlenen en significante aankopen goed te keuren kan een effectieve interne beheersingsmaatregel bieden over significante rekeningsaldi en transacties.

A157. Het kan minder praktisch uitvoerbaar zijn om functiescheiding in minder complexe entiteiten met minder medewerkers tot stand te brengen. In een door de eigenaar bestuurde entiteit kan de

eigenaar-bestuurder echter mogelijk meer effectief toezicht uitoefenen door directe betrokkenheid dan bij een grotere entiteit, wat de over het algemeen beperktere mogelijkheden voor functiescheiding kan compenseren. Hoewel, zoals ook uitgelegd in ISA 240, overheersing van het management door een enkel persoon kan een potentiële tekortkoming in de interne beheersing zijn, omdat er een mogelijkheid is voor het management om de interne beheersing te doorbreken.[39]

Interne beheersingsmaatregelen die inspelen op de risico's op een afwijking van materieel belang op het niveau van beweringen (Zie par. 26(a))

Interne beheersingsmaatregelen die inspelen op risico's waarvan is bepaald dat ze een significant risico zijn (Zie par. 26(a)(i))

A158. Ongeacht of de auditor van plan is om de effectieve werking van interne beheersingsmaatregelen te toetsen die inspelen op significante risico's, kan het verkregen inzicht over de aanpak van het management om in te spelen op deze risico's een basis vormen voor de opzet en de uitvoering van gegevensgerichte werkzaamheden die inspelen op significante risico's zoals vereist door ISA 330.[40] Hoewel risico's met betrekking tot significante niet-routinematige of oordeelsvormende aangelegenheden vaak minder waarschijnlijk onderworpen zijn aan routinematige interne beheersingsmaatregelen, is het mogelijk dat het management op een andere manier op dergelijke risico's inspeelt. Dienovereenkomstig kan het inzicht van de auditor of de entiteit interne beheersingsmaatregelen heeft opgezet en geïmplementeerd voor significante risico's die voortkomen uit niet-routinematige of oordeelsvormende aangelegenheden omvatten of en hoe het management inspeelt op de risico's. De manieren om op risicio's in te spelen kunnen omvatten:

- interne beheersingsmaatregelen, zoals een beoordeling van veronderstellingen door het senior management of deskundigen;
- gedocumenteerde processen voor schattingen;
- goedkeuring door de met governance belaste personen.

Voorbeeld:
Indien er sprake is van eenmalige gebeurtenissen, zoals de ontvangst van een kennisgeving van een significante rechtszaak, kan bij het overwegen van de manier waarop de entiteit hierop heeft ingespeeld rekening worden gehouden met aangelegenheden zoals de vragen of de entiteit al dan niet geschikte deskundigen (zoals interne of externe juridisch adviseurs) heeft ingeschakeld, of een inschatting is gemaakt van de mogelijke gevolgen en hoe wordt voorgesteld om de omstandigheden toe te lichten in de financiële overzichten.

A159. ISA 240[41] vereist dat de auditor inzicht verwerft in de interne beheersingsmaatregelen met betrekking tot ingeschatte risico's op een afwijking van materieel belang als gevolg van fraude (die worden behandeld als significante risico's), en legt verder uit dat het belangrijk is voor de auditor om inzicht te verwerven in de interne beheersingsmaatregelen die het management heeft opgezet, geïmplementeerd en onderhouden om fraude te voorkomen en te detecteren.

Interne beheersingsmaatregelen over journaalboekingen (Zie par. 26(a)(ii))

A160. Interne beheersingsmaatregelen die inspelen op de risico's op een afwijking van materieel belang op het beweringenniveau die naar verwachting voor alle controles worden geïdentificeerd, zijn interne beheersingsmaatregelen over journaalboekingen. De manier waarop een entiteit informatie van transactieverwerking opneemt in het grootboek omvat normaal gesproken het gebruik van journaalboekingen, hetzij standaard of niet-standaard, of geautomatiseerd of handmatig. De mate waarin andere interne beheersingsmaatregelen worden geïdentificeerd, kan

[39] ISA 240, paragraaf A28.
[40] ISA 330, paragraaf 21.
[41] ISA 240, paragrafen 28 en A33.

variëren op basis van de aard van de entiteit en de geplande aanpak van de auditor van verdere controlewerkzaamheden.

Voorbeeld:
Bij een controle van een minder complexe entiteit is het informatiesysteem van de entiteit mogelijk niet complex en kan de auditor mogelijk niet van plan zijn om te steunen op de effectieve werking van interne beheersingsmaatregelen. Verder kan de auditor geen significante risico's of andere risico's op een afwijking van materieel belang hebben geïdentificeerd waarvoor het noodzakelijk is voor de auditor om de opzet van interne beheersingsmaatregelen te evalueren en te bepalen dat deze zijn geïmplementeerd. Bij een dergelijke controle kan de auditor bepalen dat er geen andere geïdentificeerde interne beheersingsmaatregelen zijn dan de interne beheersingsmaatregelen van de entiteit over journaalboekingen.

Geautomatiseerde hulpmiddelen en technieken

A161. Bij handmatige grootboeksystemen kunnen niet-standaard journaalboekingen mogelijk worden geïdentificeerd door inspectie van grootboeken, journaals en ondersteunende documentatie. Wanneer geautomatiseerde procedures worden gebruikt voor het bijhouden van het grootboek en het opstellen van financiële overzichten, is het mogelijk dat dergelijke boekingen alleen in elektronische vorm bestaan waardoor ze gemakkelijker zijn te identificeren door het gebruik van geautomatiseerde technieken.

Voorbeeld:
Bij de controle van een minder complexe entiteit kan de auditor mogelijk een totale lijst van alle journaalboekingen in een eenvoudige spreadsheet extraheren. Het is dan mogelijk dat de auditor de journaalboekingen sorteert door verschillende filters toe te passen, zoals valutabedrag, naam van de opsteller of beoordelaar, journaalboekingen die alleen de balans en winst - en verliesrekening verhogen, of om de vermelding aan de hand van de datum waarop de journaalboeking naar het grootboek is geboekt te bekijken om de auditor te helpen bij het opzetten van manieren van inspelen op de geïdentificeerde risico's met betrekking tot journaalposten.

Interne beheersingsmaatregelen waarvoor de auditor van plan is de effectieve werking te toetsen (Zie par. 26(a)(iii))

A162. De auditor bepaalt of er risico's op een afwijking van materieel belang op het niveau van beweringen bestaan waarvoor het niet mogelijk is om voldoende en geschikte controle-informatie te verkrijgen door gegevensgerichte werkzaamheden alleen. Van de auditor wordt vereist, in overeenstemming met ISA 330[42], om toetsingen van interne beheersingsmaatregelen op te zetten en uit te voeren die inspelen op dergelijke risico's op een afwijking van materieel belang wanneer gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen op het niveau van beweringen. Als gevolg hiervan moeten ze, wanneer dergelijke interne beheersingsmaatregelen bestaan die inspelen op deze risico's, worden geïdentificeerd en geëvalueerd.

A163. In andere gevallen, wanneer de auditor van plan is rekening te houden met de effectieve werking van interne beheersingsmaatregelen bij het bepalen van de aard, timing en omvang van gegevensgerichte werkzaamheden in overeenstemming met ISA 330, moeten dergelijke interne beheersingsmaatregelen ook worden geïdentificeerd omdat ISA 330[43] vereist dat de auditor toetsingen van die interne beheersingsmaatregelen opzet en uitvoert.

Voorbeelden:
De auditor kan van plan zijn om de effectieve werking van interne beheersingsmaatregelen te toetsen:

- over routinematige transactiestromen omdat dergelijke toetsingen effectiever of efficiënter kunnen zijn voor grote hoeveelheden homogene transacties;

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

- over de volledigheid en nauwkeurigheid van informatie die door de entiteit is geproduceerd (bijvoorbeeld interne beheersingsmaatregelen over het opstellen van door het systeem gegenereerde rapporten), om de betrouwbaarheid van die informatie te bepalen, wanneer de auditor van plan is rekening te houden met de effectieve werking van die interne beheersingsmaatregelen bij het opzetten en uitvoeren van verdere controlewerkzaamheden;
- met betrekking tot doelstellingen op het gebied van de activiteiten en de naleving van wet- en regelgeving wanneer deze betrekking hebben op gegevens die de auditor evalueert of gebruikt bij het toepassen van controlewerkzaamheden.

A164. De plannen van de auditor om de effectieve werking van interne beheersingsmaatregelen te toetsen kunnen ook worden beïnvloed door de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van de financiële overzichten. Bijvoorbeeld als tekortkomingen zijn geïdentificeerd met betrekking tot de interne beheersingsomgeving, kan dit de algemene verwachtingen van de auditor over de effectieve werking van directe interne beheersingsmaatregelen beïnvloeden.

Andere interne beheersingsmaatregelen die de auditor geschikt acht (Zie par. 26(a)(iv))

A165. Andere interne beheersingsmaatregelen die de auditor kan overwegen die geschikt zijn om de opzet te identificeren en te evalueren en om de implementatie te bepalen, kunnen omvatten:

- interne beheersingsmaatregelen die inspelen op risico's die als hoger worden ingeschat op het spectrum van inherent risico maar die niet als significant risico bepaald zijn;
- interne beheersingsmaatregelen met betrekking tot het aansluiten van gedetailleerde vastleggingen met het grootboek; of
- aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie bij gebruik van een serviceorganisatie.[44]

Identificatie van IT-applicaties en andere aspecten van de IT-omgeving, risico's die voortkomen uit het gebruik van IT en *general IT controls* (Zie par. 26(b)-(c))

Bijlage 5 bevat voorbeeldkenmerken van IT-applicaties en andere aspecten van de IT omgeving en leidraden met betrekking tot die kenmerken, die relevant kunnen zijn bij het identificeren van IT applicaties en andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT.

IT-applicaties en andere aspecten van de IT-omgeving identificeren (Zie par. 26(b))

Waarom de auditor risico's identificeert die voortkomen uit het gebruik van IT en *general IT controls* met betrekking tot geïdentificeerde IT applicaties en andere aspecten van de IT-omgeving

A166. Inzicht in de risico's die voortkomen uit het gebruik van IT en de *general IT controls* die door de entiteit zijn geïmplementeerd om in te spelen op deze risico's, kan van invloed zijn op:

- de beslissing van de auditor over het al dan niet toetsen van de effectieve werking van de interne beheersingsmaatregelen die inspelen op risico's op een afwijking van materieel belang op het niveau van beweringen;

Voorbeeld:
Wanneer *general IT controls* niet effectief zijn opgezet of niet passend zijn geïmplementeerd om in te spelen op risico's die voortkomen uit het gebruik van IT (bijvoorbeeld interne beheersingsmaatregelen voorkomen of detecteren niet op een passende manier ongeautoriseerde programmawijzigingen of ongeautoriseerde toegang tot IT-applicaties), kan dit gevolgen hebben voor de beslissing van de auditor om te steunen op geautomatiseerde interne beheersingsmaatregelen binnen de betrokken IT-applicaties.

[44] ISA 402, *Overwegingen met betrekking tot controles van entiteiten die gebruikmaken van een serviceorganisatie.*

- de inschatting door de auditor van het interne beheersingsrisico op het niveau van beweringen;

Voorbeeld:
De blijvende effectieve werking van een interne beheersingsmaatregel voor informatieverwerking kan afhangen van bepaalde *general IT controls* die ongeautoriseerde programmawijzigingen in de interne beheersingsmaatregel voor IT informatieverwerking voorkomen of detecteren (d.w.z., interne beheersingsmaatregelen inzake programmawijzigingen over de gerelateerde IT-applicatie). In dergelijke omstandigheden kan de verwachte effectieve werking (of het ontbreken daarvan) van de *general IT controls* de inschatting door de auditor van het interne beheersingsrisico beïnvloeden (het interne beheersingsrisico kan bijvoorbeeld hoger zijn wanneer wordt verwacht dat dergelijke *general IT controls* niet effectief zijn of als de auditor niet van plan is om de *general IT controls* te toetsen).

- de strategie van de auditor voor het toetsen van informatie geproduceerd door de entiteit die wordt geproduceerd door of informatie betreft uit de IT-applicaties van de entiteit;

Voorbeeld:
Wanneer door de entiteit geproduceerde informatie om te worden gebruikt als controle-informatie geproduceerd wordt door IT applicaties, kan de auditor bepalen om interne beheersingsmaatregelen over door het systeem gegenereerde rapporten te toetsen, inclusief identificatie en toetsing van de *general IT controls* die inspelen op risico's van ongepaste of ongeautoriseerde programmawijzigingen of directe gegevenswijzigingen in de rapporten.

- de inschatting door de auditor van inherent risico op het niveau van beweringen; of

Voorbeeld:
Wanneer er significante of uitgebreide programmeringswijzigingen in een IT-applicatie zijn om nieuwe of herziene rapportagevereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving te behandelen, kan dit een indicator zijn voor de complexiteit van de nieuwe vereisten en hun effect op de financiële overzichten van de entiteit. Wanneer dergelijke uitgebreide programmering of veranderingen in gegevens voorkomen, is de IT-applicatie waarschijnlijk ook onderhevig aan risico's die voortkomen uit het gebruik van IT.

- de opzet van verdere controlewerkzaamheden.

Voorbeeld:
Als interne beheersingsmaatregelen voor informatieverwerking afhangen van *general IT controls*, kan de auditor bepalen om de effectieve werking van de *general IT controls* te toetsen, wat dan de opzet van toetsingen van interne beheersingsmaatregelen voor dergelijke *general IT-controls* vereist. Als in dezelfde omstandigheden de auditor bepaalt om de effectieve werking van de *general IT controls* niet te toetsen of de *general IT controls* naar verwachting niet effectief zullen zijn, kan het nodig zijn om in te spelen op de bijbehorende risico's die voortkomen uit het gebruik van IT door het opzetten van gegevensgerichte werkzaamheden. Echter, op de risico's die voortkomen uit het gebruik van IT kan mogelijk niet worden ingespeeld wanneer dergelijke risico's verband houden met risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen. In dergelijke omstandigheden moet de auditor mogelijk de implicaties voor het controle-oordeel overwegen.

Het identificeren van IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT

A167. Voor de IT-applicaties die relevant zijn voor het informatiesysteem, kan inzicht in de aard en complexiteit van de specifieke IT-processen en *general IT controls* die de entiteit heeft, de auditor helpen bij het bepalen op welke IT-applicaties de entiteit steunt om de integriteit van informatie in het informatiesysteem van de entiteit nauwkeurig te verwerken en onderhouden. Dergelijke IT-applicaties kunnen onderhevig zijn aan risico's die voortkomen uit het gebruik van IT.

A168. Bij het identificeren van de IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT, moet rekening worden gehouden met interne beheersingsmaatregelen die door de auditor zijn geïdentificeerd omdat dergelijke controlemaatregelen het gebruik van IT of het steunen op IT kunnen inhouden. De auditor kan zich concentreren op de vraag of een IT-applicatie geautomatiseerde interne beheersingsmaatregelen omvat waarop het management steunt en die de auditor heeft geïdentificeerd, inclusief interne beheersingsmaatregelen die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen. De auditor kan ook overwegen hoe informatie wordt opgeslagen en verwerkt in het informatiesysteem met betrekking tot significante transactiestromen, rekeningsaldi en toelichtingen en of het management steunt op *general IT controls* om de integriteit van die informatie te handhaven.

A169. De door de auditor geïdentificeerde interne beheersingsmaatregelen kunnen afhankelijk zijn van door het systeem gegenereerde rapporten, in welk geval de IT applicaties die deze rapporten produceren onderhevig kunnen zijn aan risico's die voortkomen uit het gebruik van IT. In andere gevallen is het mogelijk dat de auditor niet van plan is om te steunen op interne beheersingsmaatregelen over de door het systeem gegenereerde rapporten en van plan is om direct de *inputs* en *outputs* van dergelijke rapporten te toetsen, in welk geval de auditor mogelijk niet de gerelateerde IT-applicaties identificeert als onderhevig aan risico's die voortkomen uit IT.

Schaalbaarheid

A170. De mate van inzicht van de auditor in de IT-processen, inclusief de mate waarin de entiteit beschikt over *general IT controls*, zal variëren met de aard en de omstandigheden van de entiteit en haar IT-omgeving, evenals op basis van de aard en omvang van de interne beheersingsmaatregelen die door de auditor zijn geïdentificeerd. Het aantal IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT zal ook variëren op basis van deze factoren.

Voorbeelden:

- Een entiteit die commerciële software gebruikt en geen toegang heeft tot de broncode om programmawijzigingen aan te brengen, heeft waarschijnlijk geen proces voor programmawijzigingen, maar kan een proces of procedures hebben om de software te configureren (bijvoorbeeld het rekeningschema, rapportage parameters of drempels). Bovendien kan de entiteit een proces of procedures hebben om toegang tot de applicatie te beheren (bijv. een aangewezen persoon met beheerderstoegang voor de commerciële software). In dergelijke omstandigheden is het onwaarschijnlijk dat de entiteit geformaliseerde *general IT controls* heeft of nodig heeft.
- Een grotere entiteit daarentegen kan in hoge mate op IT steunen en de IT-omgeving kan betrekking hebben op meerdere IT-applicaties en de IT-processen voor het beheer van de IT-omgeving kunnen complex zijn (er bestaat bijvoorbeeld een speciale IT-afdeling die programmawijzigingen ontwikkelt en implementeert en toegangsrechten beheert), inclusief dat de entiteit geformaliseerde general IT-control over zijn IT-processen heeft geïmplementeerd.
- Wanneer het management niet steunt op geautomatiseerde interne beheersingsmaatregelen of *general IT controls* om transacties te verwerken of de gegevens bij te houden en de auditor geen geautomatiseerde interne beheersingsmaatregelen of andere interne beheersingsmaatregelen voor informatieverwerking (of die afhankelijk zijn van *general IT controls*) heeft geïdentificeerd, kan de auditor van plan zijn om alle informatie die door de entiteit met IT is geproduceerd rechtstreeks te toetsen en kan hij mogelijk geen IT-applicaties identificeren die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT.
- Wanneer het management steunt op een IT-applicatie om gegevens te verwerken of te onderhouden, de hoeveelheid gegevens significant is en het management steunt op de IT-applicatie om geautomatiseerd interne beheersingsmaatregelen uit te voeren die de auditor ook heeft geïdentificeerd, zal de IT-applicatie waarschijnlijk onderhevig zijn aan risico's die voortkomen uit het gebruik van IT.

A171. Wanneer een entiteit een grotere complexiteit in haar IT-omgeving heeft, vereist het identificeren van de IT-applicaties en andere aspecten van de IT-omgeving, het bepalen van de gerelateerde risico's die voortkomen uit het gebruik van IT en het identificeren van *general IT-controls* waarschijnlijk de betrokkenheid van teamleden met gespecialiseerde vaardigheden in IT. Een dergelijke betrokkenheid is waarschijnlijk essentieel en moet mogelijk uitgebreid zijn voor complexe IT omgevingen.

Identificeren van andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT

A172. De andere aspecten van de IT-omgeving die onderhevig kunnen zijn aan risico's die voortkomen uit het gebruik van IT, omvatten het netwerk, besturingssysteem en databases en, in bepaalde omstandigheden, interfaces tussen IT-applicaties. Andere aspecten van de IT-omgeving worden over het algemeen niet geïdentificeerd wanneer de auditor geen IT-applicaties identificeert die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT. Wanneer de auditor IT-applicaties heeft geïdentificeerd die onderhevig zijn aan risico's die voortkomen uit IT, worden andere aspecten van de IT-omgeving (bijvoorbeeld database, besturingssysteem, netwerk) waarschijnlijk geïdentificeerd omdat dergelijke aspecten de geïdentificeerde IT-applicaties ondersteunen en daarmee interactie hebben.

Identificeren van risico's die voortkomen uit het gebruik van IT en *general IT controls* (Zie par. 26(c))

Bijlage 6 bevat overwegingen voor het verwerven van inzicht in *general IT controls*.

A173. Bij het identificeren van de risico's die voortkomen uit het gebruik van IT, kan de auditor rekening houden met de aard van de geïdentificeerde IT-applicatie of een ander aspect van de IT-omgeving en de redenen waarom risico's kunnen ontstaan uit het gebruik van IT. Voor sommige geïdentificeerde IT-applicaties of andere aspecten van de IT-omgeving, kan de auditor van toepassing zijnde risico's identificeren die voortkomen uit het gebruik van IT en die voornamelijk betrekking hebben op niet-geautoriseerde toegang of ongeautoriseerde programmawijzigingen, evenals risico's die verband houden met ongepaste gegevenswijzigingen (bijvoorbeeld het risico op ongepaste wijzigingen in de gegevens door directe databasetoegang of de mogelijkheid om informatie rechtstreeks te manipuleren).

A174. De omvang en aard van de van toepassing zijnde risico's die voortkomen uit het gebruik van IT variëren afhankelijk van de aard en kenmerken van de geïdentificeerde IT-applicaties en andere aspecten van de IT-omgeving. Van toepassing zijnde IT-risico's kunnen ontstaan wanneer de entiteit voor geïdentificeerde aspecten van zijn IT-omgeving (bijvoorbeeld het uitbesteden van de *hosting* van zijn IT-omgeving aan een derde of het gebruikmaken van een *shared service center* voor centraal beheer van IT-processen in een groep) externe of interne dienstverleners gebruikt. Van toepassing zijnde risico's die voortkomen uit het gebruik van IT kunnen ook worden geïdentificeerd met betrekking tot *cybersecurity*. Het is waarschijnlijker dat er meer risico's zullen voortkomen uit het gebruik van IT wanneer de hoeveelheid of de complexiteit van geautomatiseerde *application controls* hoger is en het management meer steunt op deze interne beheersingsmaatregelen voor de effectieve verwerking van transacties of het effectieve onderhoud van de integriteit van onderliggende informatie.

Evalueren van de opzet en het bepalen van de implementatie van geïdentificeerde interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten". (Zie par. 26(d))

A175. Bij het evalueren van de opzet van een geïdentificeerde interne beheersingsmaatregel omvat de overweging van de auditor of de interne beheersingsmaatregel, afzonderlijk of in combinatie met andere interne beheersingsmaatregelen, in staat is om effectief afwijkingen van materieel belang te voorkomen of te detecteren en corrigeren van (d.w.z. de interne beheersingsdoelstelling).

A176. De auditor bepaalt de implementatie van een geïdentificeerde interne beheersingsmaatregel door vast te stellen dat de interne beheersingsmaatregel bestaat en dat de entiteit deze toepast. Het

heeft weinig zin dat de auditor de implementatie beoordeelt van een interne beheersingsmaatregel die niet effectief is opgezet. Daarom evalueert de auditor de opzet van een interne beheersingsmaatregel eerst. Een niet-adequaat opgezette interne beheersingsmaatregel kan een tekortkoming in de interne beheersing vormen.

A177. Risico-inschattingswerkzaamheden om controle-informatie te verkrijgen over de opzet en de implementatie van geïdentificeerde interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"" kunnen omvatten:

- verzoeken om inlichtingen bij personeel van de entiteit;
- waarneming van de toepassing van specifieke interne beheersingsmaatregelen;
- inspectie van documenten en rapporten.

Verzoek om inlichtingen alleen is echter niet voldoende voor dergelijke doeleinden.

A178. De auditor kan verwachten, op basis van ervaring uit de vorige controle of op basis van de risico-inschattingswerkzaamheden in de huidige verslagperiode, dat het management geen effectieve interne beheersingsmaatregelen heeft opgezet of geïmplementeerd om in te spelen op een significant risico. In dergelijke gevallen kunnen de werkzaamheden die worden uitgevoerd om het vereiste in paragraaf 26(d) te adresseren, bestaan uit het vaststellen dat dergelijke interne beheersingsmaatregelen niet effectief zijn opgezet of geïmplementeerd. Als de resultaten van de werkzaamheden aangeven dat interne beheersingsmaatregelen nieuw zijn opgezet of geïmplementeerd, dan moet de auditor de werkzaamheden in paragraaf 26(b)-(d) uitvoeren op de nieuw opgezette of geïmplementeerde interne beheersingsmaatregelen.

A179. De auditor kan concluderen dat een interne beheersingsmaatregel, die effectief is opgezet en geïmplementeerd, geschikt kan zijn om te toetsen om rekening te houden met de effectieve werking bij het opzetten van gegevensgerichte werkzaamheden. Als een interne beheersingsmaatregel echter niet effectief is opgezet of geïmplementeerd, heeft het geen voordeel om deze te toetsen. Wanneer de auditor van plan is een interne beheersingsmaatregel te toetsen, is de informatie die verkregen is over de mate waarin de interne beheersingsmaatregel inspeelt op risico(s) op een afwijking van materieel belang, een *input* voor de risico-inschatting van de auditor van de interne beheersingsmaatregel op het niveau van beweringen.

A180. Het evalueren van de opzet en het bepalen van de implementatie van geïdentificeerde interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten" is niet voldoende om hun effectieve werking te toetsen. Voor geautomatiseerde interne beheersingsmaatregelen kan de auditor echter van plan zijn om de effectieve werking van geautomatiseerde interne beheersingsmaatregelen te toetsen door deze *general IT controls* die zorgen voor de consistente werking van een geautomatiseerde controle, te identificeren en te toetsen. Dit in plaats van het direct toetsen van de effectieve werking van de geautomatiseerde interne beheersingsmaatregelen. Het verkrijgen van controle-informatie over de implementatie van een handmatige interne beheersingsmaatregel op een bepaald tijdstip levert geen controle-informatie op over de effectieve werking van de interne beheersingsmaatregel op andere tijdstippen tijdens de gecontroleerde periode. Toetsingen van de effectieve werking van interne beheersingsmaatregelen, inclusief toetsingen van indirecte interne beheersingsmaatregelen, zijn verder beschreven in ISA 330.[45]

A181. Wanneer de auditor niet van plan is om de effectieve werking van geïdentificeerde interne beheersingsmaatregelen te toetsen, kan het verworven inzicht van de auditor nog steeds helpen bij de opzet van de aard, timing en omvang van gegevensgerichte controlewerkzaamheden die inspelen op de gerelateerde risico's op een afwijking van materieel belang.

Voorbeeld:

[45] ISA 330, paragrafen 8-11.

De resultaten van deze risico-inschattingswerkzaamheden kunnen een basis vormen voor de overweging van de auditor van mogelijke deviaties in een populatie bij het opzetten van steekproeven bij een controle.

Tekortkomingen in interne beheersing binnen het interne beheersingssysteem van de entiteit (Zie par. 27)

A182. Bij het uitvoeren van de evaluaties van elk van de componenten van het interne beheersingssysteem van de entiteit,[46] kan de auditor bepalen dat bepaalde beleidslijnen van de entiteit in een component niet geschikt zijn voor de aard en omstandigheden van de entiteit. Een dergelijke bepaling kan een indicator zijn die de auditor helpt bij het identificeren van tekortkomingen in de interne beheersing. Als de auditor een of meer tekortkomingen in de interne beheersing heeft geïdentificeerd, kan de auditor het effect van die tekortkomingen in de interne beheersing overwegen bij het opzetten van verdere controlewerkzaamheden in overeenstemming met ISA 330.

A183. Als de auditor een of meer tekortkomingen in de interne beheersing heeft geïdentificeerd, vereist ISA 265[47] van de auditor om te bepalen of de tekortkomingen, afzonderlijk of in combinatie, een significant tekortkoming vormen.

De auditor past professionele oordeelsvorming toe om te bepalen of een tekortkoming een significante tekortkoming in de interne beheersing vormt.[48]

Voorbeelden:
Omstandigheden die kunnen wijzen op een significante tekortkoming in de interne beheersing omvatten aangelegenheden zoals:

- de identificatie van fraude van elke omvang waarbij het senior management betrokken is;
- geïdentificeerde interne processen die inadequaat zijn met betrekking tot de rapportage en communicatie van tekortkomingen die zijn opgemerkt door de interne audit;
- eerder gecommuniceerde tekortkomingen die niet tijdig door het management worden gecorrigeerd;
- het niet inspelen door het management op significante risico's, bijvoorbeeld door geen interne beheersingsmaatregelen te implementeren over significante risico's; en
- de aanpassing van eerder gepubliceerde financiële overzichten.

De risico's op een afwijking van materieel belang identificeren en inschatten (Zie par. 28-37)

Waarom de auditor de risico's op een afwijking van materieel belang identificeert en inschat

A184. Risico's op een afwijking van materieel belang worden geïdentificeerd en ingeschat door de auditor om de aard, timing en omvang van verdere controlewerkzaamheden die nodig zijn om voldoende en geschikte controle-informatie te verkrijgen, te bepalen. Deze informatie stelt de auditor in staat om een oordeel geven over de financiële overzichten bij een aanvaardbaar laag niveau van controlerisico.

A185. Informatie die wordt verzameld door het uitvoeren van risico-inschattingswerkzaamheden wordt gebruikt als controle-informatie om de basis voor de identificatie en inschatting van de risico's op een afwijking van materieel belang te verschaffen. De controle-informatie verkregen bij het evalueren van de opzet van geïdentificeerde interne beheersingsmaatregelen en het bepalen of die interne beheersingsmaatregelen zijn geïmplementeerd in de component "interne beheersingsactiviteiten", wordt bijvoorbeeld als controle-informatie gebruikt om de risico-

[46] Paragrafen 21(b), 22(b), 24(c), 25(c) en 26(d).
[47] ISA 265, *Meedelen van tekortkomingen in de interne beheersing aan de met governance belaste personen en het management*, paragraaf 8.
[48] ISA 265, paragrafen A6-A7 beschrijven indicatoren van significante tekortkomingen en zijn van belang om te bepalen of een tekort, of een combinatie van tekortkomingen, in de interne beheersing vormt een significant tekort.

inschatting te ondersteunen. Dergelijke informatie biedt ook een basis voor de auditor om algehele manieren op te zetten om in te spelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van de financiële overzichten, evenals het opzetten en uitvoeren van verdere controlewerkzaamheden waarvan de aard, timing en omvang inspelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van beweringen, in overeenstemming met ISA 330.

Identificeren van risico's op een afwijking van materieel belang (Zie par. 28)

A186. De identificatie van risico's op een afwijking van materieel belang wordt uitgevoerd voordat rekening wordt gehouden met eventuele daarop betrekking hebbende interne beheersingsmaatregelen (d.w.z. het inherente risico) en is gebaseerd op de voorlopige overweging van de auditor van afwijkingen die een redelijke mogelijkheid hebben om zowel voor te komen als om van materieel belang te zijn als ze voorkomen.[49]

A187. Het identificeren van de risico's op een afwijking van materieel belang vormt ook de basis voor de vaststelling door de auditor van relevante beweringen, die de auditor helpen bij het bepalen van de significante transactiestromen, rekeningsaldi en toelichtingen.

Beweringen

Waarom de auditor beweringen gebruikt

A188. Bij het identificeren en inschatten van de risico's op een afwijking van materieel belang gebruikt de auditor beweringen om rekening houden met de verschillende soorten potentiële afwijkingen die kunnen voorkomen. Beweringen waarvoor de auditor gerelateerde risico's op een afwijking van materieel belang heeft geïdentificeerd, zijn relevante beweringen.

Het gebruik van beweringen

A189. Bij het identificeren en inschatten van de risico's op een afwijking van materieel belang kan de auditor de categorieën van beweringen gebruiken zoals beschreven in paragraaf A190 (a)-(b) hieronder of kan deze anders weergeven mits alle hieronder beschreven aspecten zijn behandeld. De auditor kan ervoor kiezen om de beweringen over transactiestromen en gebeurtenissen en daarop betrekking hebbende toelichtingen te combineren met de beweringen over rekeningsaldi en daarop betrekking hebbende toelichtingen.

A190. Beweringen die door de auditor worden gebruikt bij het overwegen van de verschillende soorten potentiële afwijkingen die kunnen voorkomen, kunnen in de volgende categorieën vallen:

(a) beweringen over transactiestromen en gebeurtenissen en daarop betrekking hebbende toelichtingen tijdens de gecontroleerde periode:

(i) voorkomen – de vastgelegde of toegelichte transacties en gebeurtenissen hebben inderdaad plaatsgevonden en dergelijke transacties en gebeurtenissen hebben betrekking op de entiteit;
(ii) volledigheid – alle transacties en gebeurtenissen die hadden moeten worden vastgelegd, zijn ook vastgelegd en alle daarop betrekking toelichtingen die hadden moeten worden opgenomen in de financiële overzichten, zijn opgenomen;
(iii) nauwkeurigheid – bedragen en andere gegevens die betrekking hebben op vastgelegde transacties en gebeurtenissen zijn op de juiste wijze vastgelegd en daarop betrekking hebbende toelichtingen zijn op de juiste wijze vastgelegd en beschreven;
(iv) afgrenzing – transacties en gebeurtenissen zijn in de juiste verslagperiode vastgelegd;
(v) classificatie – transacties en gebeurtenissen zijn op de juiste rekeningen vastgelegd;

[49] ISA 200, paragraaf A16.

(vi) presentatie – transacties en gebeurtenissen zijn op de juiste wijze samengevoegd of uitgesplitst en duidelijk beschreven, en daarop betrekking hebbende toelichtingen zijn relevant en begrijpelijk in de context van de vereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving;

(b) beweringen over rekeningsaldi en daarop betrekking hebbende toelichtingen aan het einde van de verslagperiode:

(i) bestaan-activa, passiva en eigenvermogensbelangen bestaan;
(ii) rechten en verplichtingen – de entiteit bezit of heeft zeggenschap over de rechten op activa, en de verplichtingen zijn de verplichtingen voor de entiteit;
(iii) volledigheid – alle activa, passiva en eigenvermogensbelangen die hadden moeten worden vastgelegd, zijn ook vastgelegd en alle daarop betrekking hebbende toelichtingen die hadden moeten worden opgenomen in de financiële overzichten, zijn ook opgenomen;
(iv) nauwkeurigheid, waardering en toerekening – activa, passiva en eigenvermogensbelangen zijn voor de juiste bedragen in de financiële overzichten opgenomen en de daaruit voortvloeiende waarderings- en toerekeningscorrecties zijn juist vastgelegd en daarop betrekking hebbende toelichtingen zijn juist vastgelegd en beschreven;
(v) classificatie-activa – passiva en eigenvermogensbelangen zijn vastgelegd op de juiste rekeningen;
(vi) presentatie-activa – passiva en eigenvermogensbelangen zijn op juiste wijze samengevoegd of uitgesplitst en duidelijk beschreven en daarop betrekking hebbende toelichtingen zijn relevant en begrijpelijk in de context van de vereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving.

A191. De beweringen beschreven in paragraaf A190(a)-(b) hierboven, zo nodig aangepast, kunnen ook worden gebruikt door de auditor bij het overwegen van de verschillende soorten afwijkingen die kunnen voorkomen in toelichtingen die niet direct verband houden met vastgelegde transactiestromen, gebeurtenissen of rekeningsaldi.

Voorbeeld:
Als voorbeeld van een dergelijke toelichting, kan van de entiteit vereist worden door het van toepassing zijnde stelsel inzake financiële verslaggeving om zijn blootstelling aan risico's die voortkomen uit financiële instrumenten te beschrijven, inclusief hoe de risico's ontstaan; de doelstellingen, beleidslijnen en processen voor het beheren van de risico's; en de methoden die worden gebruikt om de risico's te meten.

Overwegingen specifiek voor entiteiten in de publieke sector

A192. Bij het maken van beweringen over de financiële overzichten van entiteiten in de publieke sector, in aanvulling op die beweringen die uiteengezet zijn in paragraaf A190(a)-(b), kan het management vaak beweren dat transacties en gebeurtenissen zijn uitgevoerd in overeenstemming met wet- en regelgeving of andere van kracht zijnde voorschriften. Dergelijke beweringen kunnen binnen de reikwijdte van de controle van de financiële overzichten vallen.

Risico's op een afwijking van materieel belang op het niveau van de financiële overzichten (Zie par. 28(a) en 30)

Waarom de auditor risico's op een afwijking van materieel belang op het niveau van de financiële overzichten identificeert en inschat

A193. De auditor identificeert de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten om te bepalen of de risico's een diepgaande invloed hebben op de

financiële overzichten en daarom een algehele manier van inspelen vereisen in overeenstemming met ISA 330.[50]

A194. Bovendien kunnen risico's op een afwijking van materieel belang op het niveau van de financiële overzichten ook individuele beweringen beïnvloeden en het identificeren van deze risico's kan de auditor helpen bij het inschatten van risico's op een afwijking van materieel belang op het niveau van beweringen en bij het opzetten van verdere controlewerkzaamheden om in te spelen op de geïdentificeerde risico's.

Het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten

A195. Risico's op een afwijking van materieel belang op het niveau van de financiële overzichten betreffen risico's die een diepgaande invloed hebben op de financiële overzichten als geheel en hebben mogelijk invloed op een groot aantal beweringen. Risico's van deze aard zijn niet noodzakelijkerwijs risico's die in verband kunnen worden gebracht met specifieke beweringen op het niveau van transactiestromen, rekeningsaldi of toelichtingen (bijv. het risico dat het management de interne beheersingsmaatregelen doorbreekt). Ze vertegenwoordigen eerder omstandigheden die de risico's op een afwijking van materieel belang op het niveau van beweringen diepgaand kunnen vergroten. De evaluatie door de auditor van de vraag of geïdentificeerde risico's diepgaand verband houden met de financiële overzichten ondersteunt de inschatting door de auditor van de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten. In andere gevallen kan een aantal beweringen ook worden geïdentificeerd als vatbaar voor het risico en kan daarom van invloed zijn op de risico-identificatie en inschatting van de auditor van risico's op een afwijking van materieel belang op het niveau van beweringen.

Voorbeeld:
De entiteit wordt geconfronteerd met operationele verliezen en liquiditeitsproblemen en is afhankelijk van financiering die nog niet is veilig gesteld. In een dergelijke omstandigheid kan de auditor bepalen dat de continuïteitsveronderstelling aanleiding geeft tot een risico op een afwijking van materieel belang op het niveau van de financiële overzichten. In deze situatie moet het stelsel inzake financiële verslaggeving mogelijk worden toegepast met gebruik van een liquidatiebasis wat waarschijnlijk invloed zal hebben op alle beweringen.

A196. De identificatie en inschatting door de auditor van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten, wordt beïnvloed door het inzicht van de auditor in het interne beheersingssysteem van de entiteit, in het bijzonder het inzicht van de auditor in de interne beheersingsomgeving, het risico-inschattingsproces van de entiteit en het proces van de entiteit om het systeem van interne beheersing te monitoren, en:

- het resultaat van de bijbehorende evaluaties vereist op grond van paragrafen 21(b), 22(b), 24(c) en 25(c); en
- eventuele tekortkomingen in de interne beheersing die zijn geïdentificeerd in overeenstemming met paragraaf 27.

In het bijzonder kunnen risico's op het niveau van de financiële overzichten voortkomen uit tekortkomingen in de interne beheersingsomgeving of uit externe gebeurtenissen of omstandigheden zoals verslechterende economische omstandigheden.

A197. Risico's op een afwijking van materieel belang als gevolg van fraude kunnen met name relevant zijn voor de overweging van de auditor van de risico's op een afwijking van materieel belang op het niveau van de financiële overzichten.

[50] ISA 330, paragraaf 5.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

Voorbeeld:
De auditor begrijpt uit verzoeken om inlichtingen bij het management dat de financiële overzichten van de entiteit gebruikt worden in besprekingen met kredietverschaffers om verdere financiering veilig te stellen om werkkapitaal te behouden. De auditor kan daarom bepalen dat er een grotere vatbaarheid voor afwijkingen is vanwege frauderisicofactoren die het inherente risico beïnvloeden (d.w.z. de vatbaarheid van de financiële overzichten voor afwijkingen van materieel belang vanwege het risico op frauduleuze financiële verslaggeving, zoals te hoge opgave van activa en opbrengsten en te lage opgave van verplichtingen en kosten om ervoor te zorgen dat financiering zal worden verkregen).

A198. Het inzicht van de auditor, inclusief de bijbehorende evaluaties, van de interne beheersingsomgeving en andere componenten van het systeem van interne beheersing kunnen twijfels doen rijzen over de mogelijkheid van de auditor om controle-informatie te verkrijgen waarop het controleoordeel kan worden gebaseerd of kan reden zijn om de opdracht terug te geven indien dat onder de van toepassing zijnde wet- of regelgeving mogelijk is.

Voorbeelden:
- Als gevolg van de evaluatie van de interne beheersingsomgeving van de entiteit kunnen de twijfels van de auditor over de integriteit van het management van de entiteit zo ernstig zijn dat de auditor tot de conclusie komt dat het risico dat het management in de financiële overzichten een opzettelijke onjuiste voorstelling van zaken geeft dermate groot is dat geen controle kan worden uitgevoerd.
- Als gevolg van het evalueren van het informatiesysteem en de communicatie van de entiteit, bepaalt de auditor dat significante wijzigingen in de IT-omgeving slecht zijn beheerd met weinig toezicht van het management en de met governance belaste personen. De auditor concludeert dat er significante twijfels zijn over de toestand en betrouwbaarheid van de administratieve vastleggingen van de entiteit. In dergelijke omstandigheden kan de auditor bepalen dat het onwaarschijnlijk is dat voldoende en geschikte controle-informatie beschikbaar zal zijn ter onderbouwing van een goedkeurend oordeel over de financiële overzichten.

A199. ISA 705 [51] stelt eisen vast en geeft leidraden bij het bepalen of het nodig is voor de auditor om een gekwalificeerd oordeel te geven of een oordeelonthouding af te geven of, indien vereist in sommige gevallen, om de opdracht terug te geven indien dat onder de van toepassing zijnde wet of regelgeving mogelijk is.

Overwegingen specifiek voor entiteiten in de publieke sector

A200. Voor entiteiten in de publieke sector kan de identificatie van risico's op het niveau van de financiële overzichten overweging van aangelegenheden omvatten die verband houden met het politieke klimaat, het publieke belang en de programma gevoeligheid.

Risico's op een afwijking van materieel belang op het niveau van beweringen (Zie par. 28(b))

Bijlage 2 geeft voorbeelden, in de context van inherente risicofactoren, van gebeurtenissen of omstandigheden die kunnen duiden op een vatbaarheid voor afwijkingen die van materieel belang kunnen zijn.

A201. Risico's op afwijkingen van materieel belang die niet diepgaand betrekking hebben op de financiële overzichten zijn risico's op afwijkingen van materieel belang op het niveau van beweringen.

Relevante beweringen en significante transactiestromen, rekeningsaldi en toelichtingen (Zie par. 29)

[51] ISA 705, *Aanpassingen van het oordeel in de controleverklaring van de onafhankelijke auditor.*

Waarom relevante beweringen en significante transactiestromen, rekeningsaldi en toelichtingen worden bepaald

A202. Bepaling van relevante beweringen en de significante transactiestromen, rekeningsaldi en toelichtingen vormen de basis voor de reikwijdte van het inzicht van de auditor in het informatiesysteem van de entiteit zoals vereist om te worden verkregen in overeenstemming met paragraaf 25(a). Dit inzicht kan de auditor verder helpen bij het identificeren en inschatten van risico's op een afwijking van materieel belang (zie par. A86).

Geautomatiseerde hulpmiddelen en technieken

A203. De auditor kan geautomatiseerde technieken gebruiken om te helpen bij de identificatie van significante transactiestromen, rekeningsaldi en toelichtingen.

Voorbeelden:

- Een volledige populatie van transacties kan worden geanalyseerd met gebruik van geautomatiseerde hulpmiddelen en technieken om hun aard, bron, grootte en hoeveelheid te begrijpen. Door geautomatiseerde technieken toe te passen, kan de auditor bijvoorbeeld identificeren dat een rekening met een nul-saldo aan het einde van de verslagperiode bestond uit talrijke compenserende transacties en journaalboekingen die plaatsvonden tijdens de verslagperiode, wat aangeeft dat het rekeningsaldo of de transactiestroom significant kan zijn (bijvoorbeeld een salarisrekening). Deze zelfde salarisrekening kan ook onkostenvergoedingen aan het management (en andere werknemers) identificeren, die een significante toelichting kunnen zijn als gevolg van deze betalingen aan verbonden partijen.
- Door de stromen van een hele populatie van opbrengsttransacties te analyseren, kan de auditor eenvoudiger een significante transactiestroom identificeren die nog niet eerder was geïdentificeerd.

Toelichtingen die significant kunnen zijn

A204. Significante toelichtingen omvatten zowel kwantitatieve als kwalitatieve toelichtingen waarvoor er een of meer relevante beweringen zijn. Voorbeelden van toelichtingen die kwalitatieve aspecten hebben en die mogelijk relevante beweringen hebben en die daarom door de auditor als significant kunnen worden beschouwd, omvatten toelichtingen over:

- liquiditeits- en schuldconvenanten van een entiteit in financiële nood;
- gebeurtenissen of omstandigheden die hebben geleid tot de opname van een bijzondere waardevermindering;
- belangrijkste bronnen van schattingsonzekerheid, inclusief veronderstellingen over de toekomst;
- de aard van een wijziging in de grondslagen voor financiële verslaggeving en andere relevante toelichtingen vereist door het van toepassing zijnde stelsel inzake financiële verslaggeving, waar bijvoorbeeld nieuwe vereisten inzake financiële verslaggeving naar verwachting een significante invloed op de financiële positie en de financiële prestaties van de entiteit zullen hebben;
- op aandelen gebaseerde betalingsregelingen, inclusief informatie over hoe alle opgenomen bedragen werden bepaald, en andere relevante toelichtingen;
- verbonden partijen en transacties met verbonden partijen;
- gevoeligheidsanalyse, inclusief de effecten van veranderingen in veronderstellingen die in de waarderingsmethoden van de entiteit gebruikt worden met de bedoeling om gebruikers in staat te stellen de onderliggende waarderingsonzekerheid van een vastgelegd of toegelicht bedrag te begrijpen.

Inschatting van risico's op een afwijking van materieel belang op het niveau van beweringen

Inschatting van het inherente risico (Zie par. 31-33)

Inschatting van de waarschijnlijkheid en de orde van grootte van een afwijking (Zie par. 31)

Waarom de auditor de waarschijnlijkheid en de orde van grootte van een afwijking inschat

A205. De auditor beoordeelt de waarschijnlijkheid en de orde van grootte van afwijkingen voor geïdentificeerde risico's op een afwijking van materieel belang omdat de significantie van de combinatie van de waarschijnlijkheid dat een afwijking voorkomt en de orde van grootte van de mogelijke afwijking waar de afwijking zou voorkomen, bepaalt waar op het spectrum van het inherente risico het geïdentificeerde risico wordt ingeschat, hetgeen de opzet van verdere controlewerkzaamheden van de auditor om in te spelen op risico's aangeeft.

A206. Het inschatten van het inherente risico op geïdentificeerde risico's op een afwijking van materieel belang helpt de auditor ook bij het bepalen van significante risico's. De auditor bepaalt significante risico's omdat specifieke manieren van inspelen op significante risico's vereist zijn in overeenstemming met ISA 330 en andere ISA's.

A207. Inherente risicofactoren beïnvloeden de inschatting van de auditor van de waarschijnlijkheid en de orde van grootte van afwijking voor de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen. Hoe groter de mate waarin een transactiestroom, rekeningsaldo of toelichting gevoelig is voor een afwijking van materieel belang, hoe hoger de inherente risico-inschatting waarschijnlijk is. Overwegen van de mate waarin inherente risicofactoren de vatbaarheid van een bewering voor afwijking beïnvloeden, helpt de auditor bij een passende inschatting van het inherente risico voor risico's op een afwijking van materieel belang op het niveau van beweringen en in een preciezere manier van inspelen op een dergelijk risico.

Spectrum van inherent risico

A208. Bij het inschatten van het inherente risico past de auditor professionele oordeelsvorming toe bij het bepalen van de significantie van de combinatie van de waarschijnlijkheid en de orde van grootte van een afwijking.

A209. Het ingeschatte inherente risico met betrekking tot een bepaald risico op een afwijking van materieel belang op het niveau van beweringen vertegenwoordigt een oordeelsvorming binnen een interval van lager naar hoger over het spectrum van inherent risico. De oordeelsvorming over waar in het interval het inherente risico wordt ingeschat, kan variëren op basis van de aard, omvang en complexiteit van de entiteit en houdt rekening met de geschatte waarschijnlijkheid en orde van grootte van de afwijkingen en inherente risicofactoren.

A210. Bij het overwegen van de waarschijnlijkheid van een afwijking, overweegt de auditor de mogelijkheid dat er een afwijking kan voorkomen, rekening houdend met de inherente risicofactoren.

A211. Bij het overwegen van de orde van grootte van een afwijking beschouwt de auditor de kwalitatieve en kwantitatieve aspecten van de mogelijke afwijking (d.w.z. afwijkingen in beweringen over transactiestromen, rekeningsaldi of toelichtingen kunnen als van materieel belang worden beoordeeld vanwege de omvang, aard of omstandigheden).

A212. De auditor gebruikt de significantie van de combinatie van de waarschijnlijkheid en de orde van grootte van een mogelijke afwijking bij het bepalen waar op het spectrum van inherent risico (d.w.z. het interval) het inherente risico is ingeschat. Hoe hoger de combinatie van waarschijnlijkheid en orde van grootte, hoe hoger de inschatting van inherent risico; hoe lager de combinatie van waarschijnlijkheid en omvang, hoe lager de inschatting van inherent risico.

A213. Voor een risico dat als hoger wordt ingeschat op het spectrum van inherent risico, betekent dit niet dat zowel omvang als waarschijnlijkheid als hoog moeten worden ingeschat. Het is eerder het kruispunt van de grootte en waarschijnlijkheid van de afwijking van materieel belang in het

spectrum van inherent risico dat zal bepalen of het ingeschatte inherente risico hoger of lager is in het spectrum van inherent risico. Een hogere inherente risico-inschatting kan ook voortkomen uit verschillende combinaties van waarschijnlijkheid en omvang. Een hogere inherente risico-inschatting zou bijvoorbeeld kunnen resulteren uit een lagere waarschijnlijkheid maar een zeer hoge omvang.

A214. Om geschikte strategieën te ontwikkelen om te reageren op risico's op een afwijking van materieel belang, kan de auditor risico's op een afwijking van materieel belang aanduiden binnen categorieën in het spectrum van inherent risico, op basis van hun inschatting van inherent risico. Deze categorieën kunnen op verschillende manieren worden beschreven. Ongeacht de gebruikte methode van categorisatie, is de inschatting door de auditor van inherent risico passend wanneer de opzet en de uitvoering van verdere controlewerkzaamheden om de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen te behandelen, adequaat inspelen op de inschatting van inherent risico en de redenen voor die inschatting.

Risico's met een diepgaande invloed op een afwijking van materieel belang op het niveau van beweringen (Zie par. 31(b))

A215. Bij het inschatten van de geïdentificeerde risico's op een afwijking van materieel belang op het niveau van beweringen, kan de auditor concluderen dat sommige risico's op een afwijking van materieel belang meer diepgaand verband houden met de financiële overzichten als geheel en mogelijk van invloed zijn op een groot aantal beweringen, in welk geval de auditor de identificatie van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten bijwerkt.

A216. In omstandigheden waarin risico's op een afwijking van materieel belang worden geïdentificeerd als risico's op het niveau van de financiële overzichten vanwege hun diepgaande invloed op een aantal beweringen en identificeerbaar zijn met specifieke beweringen, is van de auditor vereist om rekening houden met die risico's bij het inschatten van het inherente risico voor risico's op een afwijking van materieel belang op het niveau van beweringen.

Overwegingen specifiek voor entiteiten in de publieke sector

A217. Bij het uitoefenen van professionele oordeelsvorming over de inschatting van het risico op een afwijking van materieel belang, kunnen auditors in de publieke sector rekening houden met de complexiteit van de voorschriften en leidraden, en met de risico's op niet-naleving van autoriteiten.

Significante risico's (Zie par. 32)

Waarom significante risico's worden bepaald en de implicaties voor de controle

A218. De bepaling van significante risico's stelt de auditor in staat om meer aandacht te richten op die risico's die zich aan de bovengrens van het spectrum van inherent risico bevinden door de uitvoering van bepaalde vereiste manieren van inspelen, waaronder:

- interne beheersingsmaatregelen die inspelen op significante risico's, moeten worden geïdentificeerd in overeenstemming met paragraaf 26(a)(i), met een vereiste om te evalueren of de interne beheersingsmaatregel effectief is opgezet en geïmplementeerd in overeenstemming met paragraaf 26(d);
- ISA 330 vereist dat interne beheersingsmaatregelen die inspelen op significante risico's, worden getoetst in de huidige verslagperiode (wanneer de auditor voornemens is te steunen op de effectieve werking van dergelijke interne beheersingsmaatregelen) en om gegevensgerichte werkzaamheden te plannen en uit te voeren die specifiek inspelen op het geïdentificeerde significante risico[52];

[52] ISA 330, paragrafen 15 en 21.

- ISA 330 vereist dat de auditor meer overtuigende controle-informatie verkrijgt naarmate de risico-inschatting van de auditor hoger is[53];
- ISA 260 vereist communicatie met de met governance belaste personen over de significante risico's geïdentificeerd door de auditor[54];
- ISA 701 vereist dat de auditor bij het bepalen van significante risico's rekening houdt met die aangelegenheden die significante aandacht van de auditor vereisten, hetgeen aangelegenheden zijn die kernpunten van controle kunnen zijn[55];
- tijdige beoordeling van controledocumentatie door de opdrachtpartner in de geschikte fasen tijdens de controle staat toe dat significante aangelegenheden, waaronder significante risico's, tijdig kunnen worden opgelost tot tevredenheid van de opdrachtpartner op of vóór de datum van de controleverklaring[56];
- ISA 600 (herzien) vereist van de groepsauditor om de geschiktheid te evalueren van de opzet en de uitvoering van verdere controlewerkzaamheden voor gebieden met hoger ingeschatte risico's op een afwijking van materieel belang in de financiële overzichten van een groep, of significante risico's, waarvoor een auditor van een groepsonderdeel de verdere uit te voeren controlewerkzaamheden bepaaltmeer betrokkenheid van de opdrachtpartner op groepsniveau als het significante risico betrekking heeft op een groepsonderdeel in een groepscontrole en voor het opdrachtteam op groepsniveau om het vereiste werk bij het groepsonderdeel door de accountant van het groepsonderdeel te sturen.[57].

Bepaling van significante risico's

A219. Bij het bepalen van significante risico's kan de auditor eerst die ingeschatte risico's op een afwijking van materieel belang identificeren die hoger zijn ingeschat op het spectrum van inherent risico om de basis te vormen voor het overwegen welke risico's dicht bij de bovengrens kunnen liggen. Dit zal verschillen van entiteit tot entiteit, en zal niet noodzakelijk hetzelfde zijn voor een entiteit verslagperiode op verslagperiode. Het kan afhankelijk zijn van de aard en omstandigheden van de entiteit waarvoor het risico ingeschat wordt.

A220. De bepaling van welke van de ingeschatte risico's op een afwijking van materieel belang dicht bij de bovengrens van het spectrum van inherent risico ligt, en daarom significante risico's zijn, is een kwestie van professionele oordeelsvorming, tenzij het risico moet worden behandeld als een significant risico in overeenstemming met de vereisten van een andere ISA. ISA 240 biedt verdere vereisten en leidraden met betrekking tot de identificatie en inschatting van de risico's op een afwijking van materieel belang als gevolg van fraude.[58]

Voorbeeld:
Gewoonlijk wordt contant geld bij een supermarkt als een grote waarschijnlijkheid op mogelijke afwijkingen bepaald (vanwege het risico dat geld wordt verduisterd), maar de omvang is meestal erg laag (vanwege de lage niveaus van fysiek contant geld verwerkt in de winkels). De combinatie van deze twee factoren op het spectrum van inherent risico zou er waarschijnlijk niet toe leiden om het bestaan van contanten als een significant risico te bepalen.
Een entiteit is in onderhandeling om een bedrijfssegment te verkopen. De auditor overweegt het effect op bijzondere waardevermindering van goodwill, en kan bepalen dat er een grotere waarschijnlijkheid is op mogelijke afwijking en een grotere omvang als gevolg van de impact van inherente risicofactoren van subjectiviteit, onzekerheid en vatbaarheid voor tendentie bij het management of andere frauderisicofactoren. Dit kan ertoe leiden dat een bijzondere waardevermindering van goodwill als een significant risico wordt aangemerkt.

[53] ISA 330, paragraaf 7(b).
[54] ISA 260 (herzien), paragraaf 15.
[55] ISA 701, *Communicatie van kernpunten van de controle in de controleverklaring van de onafhankelijke auditor,* paragraaf 9.
[56] ISA 220 (herzien), paragrafen 32 en A87-A89.
[57] ISA 600 (herzien), paragrafen 42.
[58] ISA 240, paragrafen 26-28.

A221. De auditor houdt bij de inschatting ook rekening met de relatieve effecten van inherente risicofactoren bij het inschatten van inherent risico. Hoe lager het effect van inherente risicofactoren, hoe lager het ingeschatte risico waarschijnlijk zal zijn. Risico's op een afwijking van materieel belang die kunnen worden ingeschat als zijnde een hoger inherent risico en kunnen daarom als een significant risico worden beschouwd. Deze kunnen dit voortkomen uit aangelegenheden als:

- transacties waarvoor meerdere aanvaardbare wijzen van administratieve verwerking bestaan, zodat subjectiviteit is betrokken;
- schattingen met een hoge schattingsonzekerheid of complexe modellen;
- complexiteit in gegevensverzameling en -verwerking ter ondersteuning van rekeningsaldi;
- rekeningsaldi of kwantitatieve toelichtingen met complexe berekeningen;
- verslaggevingsprincipes die mogelijk op verschillende manieren worden geïnterpreteerd;
- wijzigingen in de bedrijfsactiviteiten van de entiteit die veranderingen in de administratieve verwerking met zich meebrengen, bijvoorbeeld fusies en overnames.

Risico's waarvoor gegevensgerichte werkzaamheden alleen geen voldoende en geschikte controle-informatie verschaffen (Zie par. 33)

Waarom risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie verschaffen, moeten worden geïdentificeerd

A222. Vanwege de aard van een risico op een afwijking van materieel belang en de interne beheersingsactiviteiten die inspelen op dat risico, is in sommige omstandigheden het toetsen van de effectieve werking van interne beheersingsmaatregelen de enige manier om voldoende en geschikte controle-informatie te verkrijgen. Dienovereenkomstig is er een vereiste voor de auditor om dergelijke risico's te identificeren vanwege de implicaties voor de opzet en de uitvoering van verdere controlewerkzaamheden in overeenstemming met ISA 330 om in te spelen op risico's op een afwijking van materieel belang op het niveau van beweringen.

A223. Paragraaf 26(a)(iii) vereist ook de identificatie van interne beheersingsmaatregelen die inspelen op risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie kunnen verschaffen omdat van de auditor wordt vereist, in overeenstemming met ISA 330[59], om dergelijke toetsingen van interne beheersingsmaatregelen op te zetten en uit te voeren.

Bepalen van risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie bieden

A224. Waar routinematige zakelijke transacties worden onderworpen aan hoog geautomatiseerde verwerking met weinig of geen handmatige interventie, is het niet altijd mogelijk om alleen gegevensgerichte werkzaamheden uit te voeren met betrekking tot het risico. Dit kan het geval zijn in omstandigheden waarin een significante hoeveelheid informatie van een entiteit alleen in elektronische vorm is geïnitieerd, vastgelegd, verwerkt of gerapporteerd zoals in een informatiesysteem dat een hoge mate van integratie in al haar IT-applicaties bevat. In dergelijke gevallen:

- is controle-informatie mogelijk alleen beschikbaar in elektronische vorm en is de toereikendheid en geschiktheid ervan gewoonlijk afhankelijk van de effectiviteit van interne beheersingsmaatregelen met betrekking tot de nauwkeurigheid en volledigheid ervan;
- is de mogelijkheid dat onjuiste tot stand wordt gebracht of gewijzigd zonder dat de fout wordt gedetecteerd mogelijk groter als geschikte interne beheersingsmaatregelen niet effectief werken.

Voorbeeld:

[59] ISA 330, paragraaf 8.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

Het is doorgaans niet mogelijk om voldoende en geschikte controle-informatie te verkrijgen met betrekking tot opbrengsten voor een telecommunicatie-entiteit alleen op basis van gegevensgerichte werkzaamheden. Dit komt omdat de informatie van oproep- of gegevensactiviteit niet bestaat in een vorm die waarneembaar is. In plaats daarvan wordt het toetsen van substantiële interne beheersingsmaatregelen meestal uitgevoerd om te bepalen dat de oorsprong en voltooiing van oproepen en gegevensactiviteit correct wordt vastgelegd (bijv. minuten van een oproep of volume van een download) en correct vastgelegd in het factureringssysteem van de entiteit.

A225. ISA 540 (herzien) biedt verdere leidraden met betrekking tot schattingen van risico's waarvoor gegevensgerichte werkzaamheden alleen niet voldoende en geschikte controle-informatie bieden.[60] In relatie tot schattingen is dit mogelijk niet beperkt tot geautomatiseerde verwerking, maar kan dit ook van toepassing zijn op complexe modellen.

*Inschatting van het interne beheersingsrisico (*Zie par. 34)

A226. De plannen van de auditor om de effectieve werking van interne beheersingsmaatregelen te toetsen zijn gebaseerd op de verwachting dat interne beheersingsmaatregelen effectief werken en dit zal de basis vormen voor de inschatting door de auditor van het interne beheersingsrisico. De aanvankelijke verwachting van de effectieve werking van interne beheersingsmaatregelen is gebaseerd op de evaluatie van de auditor van de opzet en de bepaling van de implementatie van de geïdentificeerde interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten". Zodra de auditor de effectieve werking van de interne beheersingsmaatregelen heeft getoetst in overeenstemming met ISA 330 zal de auditor de aanvankelijke verwachting over de effectieve werking van interne beheersingsmaatregelen kunnen bevestigen. Als de interne beheersingsmaatregelen niet effectief werken zoals verwacht, dan moet de auditor de controle van het interne beheersingsrisico herzien in overeenstemming met paragraaf 37.

A227. De inschatting door de auditor van het interne beheersingsrisico kan op verschillende manieren worden uitgevoerd, afhankelijk van de voorkeurscontroletechnieken of -methodologieën, en kan op verschillende manieren worden uitgedrukt.

A228. Als de auditor van plan is om de effectieve werking van interne beheersingsmaatregelen te toetsen, kan het nodig zijn om een combinatie van interne beheersingsmaatregelen te toetsen om de verwachting van de auditor dat de interne beheersingsmaatregelen effectief werken te bevestigen. De auditor kan van plan zijn om zowel directe als indirecte interne beheersingsmaatregelen te toetsen, met inbegrip van *general IT-controls*, en, zo ja, bij de inschatting van het interne beheersingsrisico rekening te houden met het gecombineerde verwachte effect van de interne beheersingsmaatregelen. Naar de mate waarin de te toetsen interne beheersingsmaatregel niet volledig inspeelt op het ingeschatte inherente risico, zal de auditor de implicaties bepalen voor de opzet van verdere controlewerkzaamheden om het controlerisico terug te brengen tot een aanvaardbaar laag niveau.

A229. Wanneer de auditor van plan is om de effectieve werking van een geautomatiseerde interne beheersingsmaatregel te toetsen, kan de auditor ook van plan zijn om de effectieve werking van de relevante *general IT-controls* die de voortdurende werking van die geautomatiseerde controle ondersteunen, te toetsen om in te spelen op de risico's die voortkomen uit het gebruik van IT en een basis vormen voor de verwachting van de auditor dat de geautomatiseerde interne beheersingsmaatregel effectief werkte gedurende de verslagperiode. Wanneer de auditor verwacht dat gerelateerde *general IT-controls* niet effectief zijn, kan deze bepaling van invloed zijn op de inschatting van de auditor van het interne beheersingsrisico op het niveau van beweringen en moeten de verdere controlewerkzaamheden van de auditor mogelijk gegevensgerichte werkzaamheden omvatten om in te spelen op de van toepassing zijnde risico's die voortkomen uit het gebruik van IT. Verdere leidraden over de werkzaamheden die de auditor kan uitvoeren in deze omstandigheden zijn vermeld in ISA 330.[61]

[60] ISA 540 (herzien), paragrafen A87-A89.
[61] ISA 330, paragrafen A29-A30.

Evalueren van de controle-informatie verkregen uit de risicoinschattingswerkzaamheden (Zie par. 35)

Waarom de auditor de controle-informatie evalueert op basis van de risico-inschattingswerkzaamheden

A230. Controle-informatie verkregen bij het uitvoeren van risico-inschattingswerkzaamheden vormt de basis voor de identificatie en inschatting van de risico's op een afwijking van materieel belang. Dit vormt de basis voor de opzet van de auditor van de aard, timing en omvang van verdere controlewerkzaamheden die inspelen op de ingeschatte risico's op een afwijking van materieel belang op het niveau van beweringen in overeenstemming met ISA 330. Dienovereenkomstig vormt de controle-informatie verkregen uit de risico-inschattingswerkzaamheden een basis voor de identificatie en inschatting van risico's op een afwijking van materieel belang als gevolg van fraude of fouten, op het niveau van de financiële overzichten en beweringen.

De evaluatie van de controle-informatie

A231. Controle-informatie uit risico-inschattingswerkzaamheden omvat zowel informatie die de beweringen van het management ondersteunt en bevestigt en alle informatie die dergelijke beweringen tegenspreekt.[62]

Een professioneel-kritische instelling

A232. Bij het evalueren van de controle-informatie uit de risico-inschattingswerkzaamheden overweegt de auditor of voldoende inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het interne beheersingssysteem van de entiteit is verkregen om de risico's op een afwijking van materieel belang te kunnen identificeren, evenals of er enige informatie is die tegenstrijdig is en die kan duiden op een risico op een afwijking van materieel belang.

Transactiestromen, rekeningsaldi en toelichtingen die niet significant zijn, maar wel van materieel belang (Zie par. 36)

A233. Zoals uitgelegd in ISA 320, worden[63] materialiteit en controlerisico in overweging genomen bij het identificeren en inschatten van de risico's op een afwijking van materieel belang in transactiestromen, rekeningsaldi en toelichtingen. De bepaling van de materialiteit door de auditor is een kwestie van professionele oordeelsvorming en wordt beïnvloed door de perceptie van de auditor van de financiële informatiebehoeften van gebruikers van de financiële overzichten.[64] Voor de doelstelling van deze ISA en paragraaf 18 van ISA 330, zijn transactiestromen, rekeningsaldi of toelichtingen van materieel belang als het weglaten, onjuist weergeven of verhullen van informatie daarover naar verwachting redelijkerwijs de economische beslissingen van gebruikers zou kunnen beïnvloeden gebaseerd op de financiële overzichten als geheel.

A234. Er kunnen transactiestromen, rekeningsaldi of toelichtingen zijn die van materieel belang zijn maar die niet zijn vastgesteld als significante transactiestromen, rekeningsaldi of toelichtingen (d.w.z. er zijn geen relevante beweringen geïdentificeerd).

Voorbeeld:
De entiteit kan een toelichting hebben over de beloning van bestuurders waarvoor de auditor geen risico op een afwijking van materieel belang heeft geïdentificeerd. De auditor kan echter bepalen dat deze toelichting van materieel belang is op basis van de overwegingen in paragraaf A233.

A235. Controlewerkzaamheden om transactiestromen, rekeningsaldi of toelichtingen te behandelen die van materieel belang zijn, maar waarvan niet is vastgesteld dat ze significant zijn, worden

[62] ISA 500, paragraaf A5.
[63] ISA 320, paragraaf A1.
[64] ISA 320, paragraaf 4.

behandeld in ISA 330.[65] Wanneer een transactiestroom, rekeningsaldo of toelichting wordt geacht significant te zijn zoals vereist door paragraaf 29, is de transactiestroom, rekeningsaldo of toelichting ook een transactiestroom, rekeningsaldo of toelichting van materieel belang voor de doeleinden van paragraaf 18 van ISA 330.

Herziening van de risico-inschatting (Zie par. 37)

A236. Tijdens de controle kan nieuwe of andere informatie onder de aandacht van de auditor komen die significant verschilt van de informatie waarop de risico-inschatting was gebaseerd.

Voorbeeld:
De risico-inschatting van de entiteit kan gebaseerd zijn op een verwachting dat bepaalde interne beheersingsmaatregelen effectief werken. Bij het uitvoeren van toetsingen van die interne beheersingsmaatregelen kan de auditor controle-informatie verkrijgen dat deze op de relevante tijdstippen tijdens de controle niet effectief werkten. Evenzo bij het uitvoeren van gegevensgerichte werkzaamheden kan de auditor afwijkingen in bedragen of frequenties detecteren die groter zijn dan consistent is met de risico-inschattingen van de auditor. In dergelijke omstandigheden kan de risico-inschatting niet de juiste omstandigheden van de entiteit weerspiegelen en kunnen de verdere geplande controlewerkzaamheden mogelijk niet effectief zijn bij het detecteren van afwijkingen van materieel belang. Paragrafen 16 en 17 van ISA 330 bieden verdere leidraden voor het evalueren van de effectieve werking van interne beheersingsmaatregelen.

Documentatie (Zie par. 38)

A237. Voor doorlopende controles kan bepaalde documentatie worden overgedragen, zo nodig bijgewerkt om veranderingen in de activiteiten of processen van de entiteit te weerspiegelen.

A238. ISA 230 geeft aan dat, onder andere overwegingen, er misschien geen standaardmanier is waarop de uitoefening van een professioneel-kritische instelling door de auditor is gedocumenteerd, de controledocumentatie niettemin informatie kan leveren over de uitoefening van een professioneel-kritische instelling van de auditor.[66] Bijvoorbeeld wanneer de controle-informatie verkregen uit risico-inschattingswerkzaamheden informatie omvat die zowel beweringen van het management bevestigt als tegenspreekt, kan de documentatie omvatten hoe de auditor evalueerde dat informatie inclusief de professionele oordeelsvorming bij het evalueren of de controle-informatie een geschikte basis biedt voor de identificatie en inschatting van de risico's op een afwijking van materieel belang door de auditor. Voorbeelden van andere vereisten in deze ISA waarvoor documentatie informatie kan leveren over de uitoefening van een professioneel-kritische instelling door de auditor zijn onder andere:

- paragraaf 13, die van de auditor vereist dat hij risico-inschattingswerkzaamheden opzet en uitvoert op een manier die niet tendeert naar het verkrijgen van controle-informatie die het bestaan van risico's kan bevestigen of om controle-informatie uit te sluiten die het bestaan van risico's kan tegenspreken;
- paragraaf 17, die een bespreking vereist onder de kernleden van het opdrachtteam van de toepassing van het van toepassing zijnde stelsel inzake financiële verslaggeving en de vatbaarheid van financiële overzichten van de entiteit voor afwijkingen van materieel belang;
- paragraaf 19(b) en 20, die van de auditor vereisen dat hij inzicht heeft in de redenen voor eventuele wijzigingen in de grondslagen voor de financiële verslaggeving van de entiteit en om te evalueren of de grondslagen voor de financiële verslaggeving van de entiteit geschikt en consistent zijn met het van toepassing zijnde stelsel inzake financiële verslaggeving;
- paragrafen 21(b), 22(b), 23(b), 24(c), 25(c), 26(d) en 27, die vereisen dat de auditor evalueert, op basis van de vereiste verkregen inzichten, of de componenten van het systeem van interne beheersing van de entiteit passend zijn bij de omstandigheden van de

[65] ISA 330, paragraaf 18.
[66] ISA 230, paragraaf A7.

entiteit, gezien de aard en complexiteit van de entiteit en om te bepalen of een of meer tekortkomingen in de interne beheersing zijn geïdentificeerd;

- paragraaf 35, die vereist dat de auditor rekening houdt met alle controle-informatie verkregen uit de risico-inschattingswerkzaamheden, hetzij bevestigend of in tegenspraak met beweringen van management en om te evalueren of de controle-informatie verkregen uit de risico-inschattingswerkzaamheden een passende basis biedt voor de identificatie en inschatting van de risico's op een afwijking van materieel belang; en
- paragraaf 36, die vereist dat de auditor, indien van toepassing, evalueert of bepaling van de auditor dat er geen risico's zijn op een afwijking van materieel belang zijn voor een materiële transactiestroom, rekeningsaldo of toelichting passend blijft.

Schaalbaarheid

A239. De manier waarop de vereisten van paragraaf 38 zijn gedocumenteerd, is voor de auditor om te bepalen met behulp van professionele oordeelsvorming.

A240. Meer gedetailleerde documentatie, die voldoende is om een ervaren auditor, die geen eerdere ervaring heeft met de controle in staat te stellen om inzicht te krijgen in de aard, timing en omvang van de uitgevoerde controlewerkzaamheden, kan nodig zijn om de beweegreden voor moeilijke oordeelsvormingen te ondersteunen.

A241. Voor de interne beheersingsmaatregelen van minder complexe entiteiten kan de vorm en omvang van documentatie eenvoudig en relatief kort zijn. De vorm en omvang van de documentatie van de auditor wordt beïnvloed door de aard, omvang en complexiteit van de entiteit en haar systeem van interne beheersing, beschikbaarheid van informatie van de entiteit en de controlemethodologie en -technologie die tijdens de controle is gebruikt. Het is niet nodig om het geheel van het inzicht van de auditor in de entiteit en aangelegenheden die daarmee verband houden te documenteren. Kernelementen[67] van inzicht die door de auditor zijn gedocumenteerd, kunnen diegenen omvatten waarop de auditor de inschatting van de risico's op een afwijking van materieel belang heeft gebaseerd. De auditor is echter niet verplicht elke inherente risicofactor waarmee rekening is gehouden bij het identificeren en inschatten van de risico's op een afwijking van materieel belang op het niveau van beweringen te documenteren.

Voorbeeld:
Bij controles van minder complexe entiteiten kan controledocumentatie van de auditor worden opgenomen in zijn documentatie van de algemene strategie en het controleplan.[68] Evenzo kunnen bijvoorbeeld de resultaten van de risico inschatting van de auditor afzonderlijk worden gedocumenteerd, of kunnen deze worden gedocumenteerd als onderdeel van de documentatie van verdere controlewerkzaamheden van de auditor.[69]

Bijlage 1

(Zie par. A61-A67)

Overwegingen voor het verwerven van inzicht in de entiteit en haar bedrijfsmodel

Deze bijlage legt de doelstellingen en reikwijdte van het bedrijfsmodel van de entiteit uit en geeft voorbeelden van aangelegenheden die de auditor kan overwegen bij het verwerven van inzicht in de activiteiten van de entiteit die kunnen worden opgenomen het bedrijfsmodel. Het inzicht van de auditor in het bedrijfsmodel van de entiteit en hoe dit wordt beïnvloed door haar bedrijfsstrategie en

[67] ISA 230, paragraaf 8.
[68] ISA 300, *Planning van een controle van financiële overzichten*, paragrafen 7, 9 en A13.
[69] ISA 330, paragraaf 28.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

bedrijfsdoelstellingen, kan de auditor helpen bij het identificeren van bedrijfsrisico's die invloed kunnen hebben op de financiële overzichten. Bovendien kan dit de auditor helpen bij het identificeren van risico's op een afwijking van materieel belang.

Doelstellingen en reikwijdte van het bedrijfsmodel van een entiteit

1. Het bedrijfsmodel van een entiteit beschrijft hoe een entiteit bijvoorbeeld haar organisatiestructuur, activiteiten of reikwijdte van activiteiten, productlijnen(inclusief concurrenten en klanten daarvan), processen, groeimogelijkheden, globalisering, wettelijke vereisten en technologieën overweegt. Het bedrijfsmodel van de entiteit beschrijft hoe de entiteit financiële of bredere waarde creëert, behoudt en vastlegt voor haar belanghebbenden.

2. Strategieën zijn de benaderingen waarmee het management plannen heeft om de doelstellingen van de entiteit te bereiken, inclusief hoe de entiteit van plan is om in te spelen op de risico's en kansen waarmee zij wordt geconfronteerd. De strategieën van een entiteit worden in de loop van de tijd door het management gewijzigd om te reageren op wijzigingen in de doelstellingen en in de interne en externe omstandigheden waarin het actief is.

3. Een beschrijving van een bedrijfsmodel omvat doorgaans:

   - De reikwijdte van de activiteiten van de entiteit, en waarom zij deze doet.
   - De structuur en schaal van de activiteiten van de entiteit.
   - De markten of geografische of demografische gebieden en delen van de waardeketen, waarin het werkt, hoe het omgaat met die markten of gebieden (hoofdproducten, klantsegmenten en distributiemethoden), en de basis waarop het concurreert.
   - De bedrijfs- of operationele processen van de entiteit (bijvoorbeeld investeringen, financiering en operationele processen) die worden ingezet bij de uitvoering van haar activiteiten, gericht op die delen van de bedrijfsprocessen die belangrijk zijn bij het creëren, behouden of vastleggen van waarde.
   - De middelen (bijvoorbeeld financiële, menselijke, intellectuele, milieu en technologische) en andere i*nputs* en relaties (bijvoorbeeld klanten, concurrenten, leveranciers en werknemers) die noodzakelijk of belangrijk zijn voor het succes ervan.
   - Hoe het bedrijfsmodel van de entiteit het gebruik van IT integreert in haar interacties met klanten, leveranciers, kredietverschaffers en andere belanghebbenden via IT-interfaces en andere technologieën.

4. Een bedrijfsrisico kan een onmiddellijk gevolg hebben voor het risico op een afwijking van materieel belang voor transactiestromen, rekeningsaldi en toelichtingen op het niveau van beweringen of het niveau van de financiële overzichten. Bijvoorbeeld het bedrijfsrisico dat voortkomt uit een significante daling van de marktwaarde van onroerend goed kan het risico op een afwijking van materieel belang die verband houdt met de bewering van de waardering voor een kredietverstrekker van leningen op middellange termijn met vastgoed als onderpand verhogen. Hetzelfde risico, met name in combinatie met een ernstige economische neergang die tegelijkertijd het onderliggende risico op levenslange kredietverliezen op de leningen verhoogt, kan echter ook gevolgen op langere termijn hebben. De resulterende netto blootstelling aan kredietverliezen kan gerede twijfel doen ontstaan over de mogelijkheid van de entiteit om haar continuïteit te handhaven. Als dit zo is, zou dit implicaties kunnen hebben voor de conclusie van het management en van de auditor met betrekking tot de geschiktheid van het gebruik van de continuïteitsveronderstelling van de entiteit en de bepaling of er een materiële onzekerheid bestaat. Of een bedrijfsrisico kan leiden tot een risico op een afwijking van materieel belang wordt daarom overwogen in het licht van de omstandigheden van de entiteit. Voorbeelden van

gebeurtenissen en omstandigheden die aanleiding kunnen geven tot het bestaan van risico's op een afwijking van materieel belang wordt vermeld in bijlage 2.

Activiteiten van de entiteit

5. Voorbeelden van aangelegenheden die de auditor kan overwegen bij het verwerven van inzicht in de activiteiten van de entiteit (opgenomen in het bedrijfsmodel van de entiteit) omvatten:

   (a) Bedrijfsactiviteiten zoals:

   - Aard van opbrengstenbronnen, producten of diensten en markten, inclusief betrokkenheid bij elektronische handel zoals verkoop- en marketingactiviteiten via internet.
   - De uitoefening van activiteiten (bijvoorbeeld productiefasen en -methoden of activiteiten blootgesteld aan milieurisico's).
   - Samenwerkingsverbanden, joint ventures en uitbesteding van activiteiten.
   - Geografische spreiding en sectorsegmentatie.
   - Locatie van productiefaciliteiten, magazijnen en kantoren, en locatie en hoeveelheden van voorraden.
   - Belangrijkste klanten en belangrijke leveranciers van goederen en diensten, arbeidsovereenkomsten (inclusief het bestaan van cao's, pensioenrechten en andere vergoedingen na uitdiensttreding, aandelenoptie- of bonusregelingen en overheidsvoorschriften met betrekking tot arbeidsaangelegenheden).
   - Activiteiten en kosten in verband met onderzoek en ontwikkeling.
   - Transacties met verbonden partijen.

   (b) Investeringen en investeringsactiviteiten zoals:

   - Geplande of recent uitgevoerde overnames of desinvesteringen.
   - Investeringen in en verkoop van effecten en leningen.
   - Kapitaalinvesteringen.
   - Investeringen in niet-geconsolideerde entiteiten, inclusief deelnemingen zonder zeggenschap, joint ventures en voor een bijzonder doel opgerichte entiteiten.

   (c) Financiering en financieringsactiviteiten zoals:

   - Eigendomsstructuur van belangrijke dochterondernemingen en verbonden entiteiten, inclusief geconsolideerde en niet-geconsolideerde structuren.
   - Structuur van de schulden en bijbehorende voorwaarden, inclusief niet in de balans opgenomen financierings-en leaseovereenkomsten.
   - Uiteindelijk gerechtigden (bijvoorbeeld lokale, buitenlandse, zakelijke reputatie en ervaring) en verbonden partijen.
   - Gebruik van afgeleide financiële instrumenten.

Aard van voor een bijzonder doel opgerichte entiteiten

6. Een voor een bijzonder doel opgerichte entiteit (ook wel *special purpose entity* of *special-purpose vehicle* genoemd) is een entiteit die doorgaans voor een beperkt en duidelijk omschreven doel wordt opgericht, zoals het aangaan van een leaseovereenkomst of een securitisatie van

financiële activa, of om onderzoeks- en ontwikkelingsactiviteiten uit te voeren. Zij kan de vorm aannemen van een vennootschap, een trust, een maatschap of een entiteit zonder rechtspersoonlijkheid. Vaak is het zo dat de entiteit namens welke de voor een bijzonder doel opgerichte entiteit tot stand is gebracht activa transfereert naar deze laatste (bijvoorbeeld als onderdeel van een transactie waarbij financiële activa van de balans worden gehaald), het recht verkrijgt om de activa van de voor een bijzonder doel opgerichte entiteit te gebruiken, of diensten uitvoert voor de voor een bijzonder doel opgerichte entiteit, terwijl andere partijen mogelijk financiering verschaffen aan de voor een bijzonder doel opgerichte entiteit. Zoals ISA 550 aangeeft, kan een voor een bijzonder doel opgerichte entiteit in bepaalde omstandigheden een verbonden partij van de entiteit zijn.[1]

7. Stelsels inzake financiële verslaggeving specificeren vaak gedetailleerde voorwaarden die geacht worden vergelijkbaar te zijn met die van zeggenschap, of omstandigheden waaronder moet worden overwogen om de voor een bijzonder doel opgerichte entiteit in de consolidatiekring op te nemen. De interpretatie van de door dergelijke stelsels gestelde vereisten vergt vaak een gedetailleerde kennis van de relevante overeenkomsten waarbij de voor een bijzonder doel opgerichte entiteit is betrokken.

Bijlage 2

(Zie par. 12(f), 19(c), A7-A8, A85-A89)

Inzicht verwerven in inherente risicofactoren

Deze bijlage geeft nadere uitleg over de inherente risicofactoren, evenals aangelegenheden die de auditor kan overwegen bij het verweven van inzicht in en toepassen van de inherente risicofactoren bij het identificeren en inschatten van de risico's op een afwijking van materieel belang op het niveau van beweringen.

De inherente risicofactoren

1. Inherente risicofactoren zijn kenmerken van gebeurtenissen of omstandigheden die de vatbaarheid van een bewering met betrekking tot een transactiestroom, rekeningsaldo of toelichting voor een afwijking beïnvloeden, die het gevolg zijn van fraude of fouten en voordat er rekening wordt gehouden met interne beheersingsmaatregelen. Dergelijke factoren kunnen kwalitatief of kwantitatief zijn en omvatten complexiteit, subjectiviteit, wijzigingen, onzekerheid of vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of andere frauderisicofactoren[1] voor zover deze inherent risico beïnvloeden. Bij het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en de grondslagen voor financiële verslaggeving van de entiteit, in overeenstemming met paragraaf 19 (a) - (b), verwerft de auditor ook inzicht in de manier waarop inherente risicofactoren van invloed zijn op de vatbaarheid van beweringen voor afwijkingen bij het opstellen van de financiële overzichten.

2. Inherente risicofactoren met betrekking tot het opstellen van informatie vereist door het van toepassing stelsel inzake financiële verslaggeving (in deze paragraaf aangeduid als "vereiste informatie") omvatten:

[1] ISA 550, paragraaf A7.
[1] ISA 240, paragrafen A24-A27.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

- *Complexiteit* - komt voort uit de aard van de informatie of de manier waarop de vereiste informatie wordt opgesteld, inclusief wanneer dergelijke opstellingsprocessen inherent moeilijker toe te passen zijn. Er kan bijvoorbeeld complexiteit ontstaan:

    - Bij het berekenen van voorzieningen voor leverancierskorting omdat het nodig kan zijn om rekening te houden met verschillende commerciële voorwaarden bij veel verschillende leveranciers of veel onderling verbonden commerciële voorwaarden die allemaal relevant zijn voor de berekening van de verschuldigde kortingen; of
    - Wanneer er veel potentiële gegevensbronnen zijn met verschillende kenmerken gebruikt bij het maken van een schatting, de verwerking van die gegevens betrekking heeft op veel met elkaar verbonden stappen en de gegevens daarom inherent moeilijker te identificeren, vast te leggen, toegang te krijgen, te begrijpen of te verwerken zijn.

- *Subjectiviteit* - komt voort uit inherente beperkingen in de mogelijkheid om vereiste informatie op een objectieve manier op te stellen, vanwege beperkingen in de beschikbaarheid van kennis of informatie, zodanig dat het management mogelijk een keuze of een subjectieve oordeelsvorming moet maken over de juiste benadering om de resulterende informatie op te nemen in de financiële overzichten. Vanwege verschillende benaderingen bij het opstellen van de vereiste informatie, zouden verschillende uitkomsten kunnen voortkomen uit de juiste toepassing van de vereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving. Naarmate beperkingen in kennis of gegevens toenemen, neemt de subjectiviteit in de oordeelsvormingen gemaakt door redelijk bekwame en onafhankelijke personen en de diversiteit in mogelijke uitkomsten van die oordeelsvormingen ook toe.
- *Wijzigingen* - Resulteren uit gebeurtenissen of omstandigheden die in de loop van de tijd van invloed zijn op de activiteiten van de entiteit of de economische, administratieve, regelgevende, sectorspecifieke of andere aspecten van de omgeving waarin zij actief is, wanneer de effecten van die gebeurtenissen of omstandigheden worden weerspiegeld in de vereiste informatie. Dergelijke gebeurtenissen of omstandigheden kunnen zich voordoen tijdens of tussen de financiële verslagperiodes in. Wijzigingen kunnen bijvoorbeeld het gevolg zijn van ontwikkelingen in de vereisten van het van toepassing zijnde stelsel inzake financiële verslaggeving, of in de entiteit en haar bedrijfsmodel, of in de omgeving waarin de entiteit actief is. Een dergelijke wijziging kan de veronderstellingen en oordeelsvormingen van het management beïnvloeden, inclusief als deze betrekking hebben op de selectie van het management van grondslagen voor financiële verslaggeving of hoe schattingen worden gemaakt of toelichtingen daarop worden bepaald.
- *Onzekerheid* - treedt op wanneer de vereiste informatie niet alleen kan worden opgesteld op basis van voldoende precieze en uitgebreide gegevens die verifieerbaar zijn door directe waarneming. In deze omstandigheden kan een aanpak nodig zijn die de beschikbare kennis toepast om de informatie op te stellen met behulp van voldoende precieze en uitgebreide waarneembare gegevens, voor zover beschikbaar, en redelijke veronderstellingen ondersteund door de meest geschikte beschikbare gegevens, wanneer dit niet het geval is. Beperkingen op de beschikbaarheid van kennis of gegevens die niet binnen de invloed van het management vallen (onderhevig aan kostenbeperkingen waar van toepassing) zijn bronnen van onzekerheid en hun effect op het opstellen van de vereiste informatie kan niet worden weggenomen. Schattingsonzekerheid ontstaat bijvoorbeeld wanneer het vereiste geldbedrag niet met precisie kan worden bepaald en de uitkomst van de schatting niet bekend is vóór de datum dat de financiële overzichten zijn voltooid.

- *Vatbaarheid voor afwijkingen als gevolg van tendentie bij het management of andere frauderisicofactoren voor zover ze inherent risico beïnvloeden* —vatbaarheid voor tendentie bij het management resulteert uit omstandigheden die vatbaarheid creëren voor opzettelijk of onopzettelijk falen door het management om neutraliteit te handhaven bij het opstellen van de informatie. Tendentie bij het management wordt vaak geassocieerd met bepaalde voorwaarden die het potentieel hebben dat het management geen neutraliteit behoudt bij het uitoefenen van oordeelsvorming (indicatoren van mogelijke tendentie bij het management), die kunnen leiden tot een afwijking van materieel belang in de informatie die frauduleus zou zijn als het opzettelijk is. Dergelijke indicatoren omvatten stimulansen of druk voor zover ze inherent risico beïnvloeden (bijvoorbeeld als gevolg van motivatie om een gewenst resultaat te bereiken, zoals een gewenste winstdoelstelling of kapitaalratio) en gelegenheid om neutraliteit niet te behouden. Factoren die relevant zijn voor de vatbaarheid voor afwijkingen als gevolg van fraude in de vorm van frauduleuze financiële verslaggeving of oneigenlijke toe-eigening van activa worden beschreven in de paragrafen A1-A5 van ISA 240.

3. Wanneer complexiteit een inherente risicofactor is, kan er een inherente behoefte aan complexere processen bij het opstellen van de informatie en dergelijke processen kunnen inherent moeilijker toe te passen zijn. Als gevolg hiervan kan het toepassen van gespecialiseerde vaardigheden of kennis vereist zijn en kan het nodig zijn om gebruik te maken van een deskundige ingeschakeld door het management.

4. Wanneer de oordeelsvorming van het management subjectiever is, kan de vatbaarheid voor afwijkingen als gevolg van tendentie bij het management, hetzij onopzettelijk of opzettelijk, ook toenemen. Bijvoorbeeld significante oordeelsvormingen van het management kunnen een rol spelen bij het maken van schattingen die zijn geïdentificeerd als dat zij hoge schattingsonzekerheid hebben en conclusies met betrekking tot methoden, gegevens en veronderstellingen kunnen onopzettelijke of opzettelijke tendentie bij het management weerspiegelen.

Voorbeelden van gebeurtenissen of omstandigheden die aanleiding kunnen geven tot het bestaan van risico's op een afwijking van materieel belang

5. Hierna volgen voorbeelden van gebeurtenissen (inclusief transacties) en omstandigheden die kunnen wijzen op de het bestaan van risico's op een afwijking van materieel belang in de financiële overzichten, op het niveau van de financiële overzichten of het niveau van beweringen. De voorbeelden van inherente risicofactoren bevatten een breed scala aan gebeurtenissen en omstandigheden; niet alle gebeurtenissen en omstandigheden zijn echter relevant voor elke controleopdracht en de lijst met voorbeelden is niet noodzakelijk volledig. De gebeurtenissen en omstandigheden zijn gecategoriseerd door de inherente risicofactor die in de gegeven omstandigheden het grootste effect kan hebben. Belangrijk is dat vanwege de onderlinge relaties tussen inherente risicofactoren, de voorbeelden van gebeurtenissen en omstandigheden waarschijnlijk ook in verschillende mate onderhevig zijn aan of beïnvloed worden door andere inherente risicofactoren.

Relevante inherent risicofactor:	Voorbeelden van gebeurtenissen of omstandigheden die kunnen wijzen op het bestaan van risico's op afwijkingen van materieel belang op het niveau van beweringen:
Complexiteit	Regelgeving: • Activiteiten die onderhevig zijn aan een hoge mate van complexe regelgeving. Bedrijfsmodel:

	• Het bestaan van complexe samenwerkingsverbanden en joint ventures. Van toepassing zijnde stelsel inzake financiële verslaggeving: • Boekhoudkundige waarderingen met complexe processen. Transacties: • Gebruik van niet in de balans opgenomen financiering, voor een bijzonder doel opgerichte entiteiten en andere complexe financieringsovereenkomsten.
Subjectiviteit	Van toepassing zijnde stelsel inzake financiële verslaggeving: • Een breed scala aan mogelijke waarderingscriteria van een schatting. Bijvoorbeeld de opname door het management van afschrijvingen of opbrengsten en kosten uit de bouw. • Selectie door het management van een waarderingstechniek of model voor niet-vlottende activa, zoals vastgoedbeleggingen.
Wijzigingen	Economische omstandigheden: • Activiteiten in regio's die economisch onstabiel zijn, bijvoorbeeld landen met significante devaluatie van valuta of sterk inflatoire economieën. Markten: • Activiteiten blootgesteld aan volatiele markten, bijvoorbeeld handel in futures. Klant verlies: • Continuïteits- en liquiditeitsproblemen, waaronder verlies van significante klanten. Sectormodel: • Veranderingen in de sector waarin de entiteit actief is. Bedrijfsmodel: • Veranderingen in de toeleveringsketen. • Nieuwe producten of diensten ontwikkelen of aanbieden, of het starten van nieuwe bedrijfsactiviteiten. Geografie • Uitbreiden naar nieuwe locaties. Structuur van de entiteit: • Veranderingen in de entiteit zoals grote overnames of reorganisaties of andere ongebruikelijke gebeurtenissen. • Entiteiten of bedrijfssegmenten die waarschijnlijk zullen worden verkocht. Personeelscompetentie: • Veranderingen in personeel op sleutelposities, waaronder vertrek van belangrijke executives IT: • Veranderingen in de IT-omgeving. • Installatie van significante nieuwe IT-systemen met betrekking tot financiële verslaggeving. Van toepassing zijnde stelsel inzake financiële verslaggeving: • Toepassing van nieuwe boekhoudkundige regels. Kapitaal: • Nieuwe beperkingen op de beschikbaarheid van kapitaal en krediet. Regelgeving: • Aanvang van onderzoeken naar de activiteiten of financiële resultaten van de entiteit door regelgevende of overheidsinstanties. • Gevolgen van nieuwe wetgeving met betrekking tot milieubescherming.
Onzekerheid	Rapportage: • Gebeurtenissen of transacties die een significante waarderingsonzekerheid met zich meebrengen, inclusief schattingen en toelichtingen daarop. • Lopende rechtszaken en voorwaardelijke verplichtingen, bijvoorbeeld garanties op verkopen, financiële garanties en milieusanering.
Gevoeligheid voor een afwijking door	Rapportage: • Gelegenheden voor management en medewerkers om deel te nemen aan frauduleuze financiële verslaggeving, inclusief het weglaten of verhullen van significante informatie in toelichtingen.

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

tendentie bij het management of andere fraude risicofactoren voor zover zij inherent risico beïnvloeden	Transacties: • Significante transacties met verbonden partijen. • Significant aantal niet-routinematige of niet-systematische transacties inclusief intercompany-transacties en transacties met grote opbrengsten aan het einde van de verslagperiode. • Transacties die worden geregistreerd op basis van de intentie van het management; bijvoorbeeld voor herfinanciering van schulden, te verkopen activa en classificatie van verhandelbare effecten.

Andere gebeurtenissen of omstandigheden die kunnen wijzen op risico's op een afwijking van materieel belang op het niveau van de financiële overzichten:

- Een tekort aan personeel met de nodige vaardigheden op het gebied van administratieve verwerking en financiële verslaggeving.
- Tekortkomingen in de interne beheersing - met name in de interne beheersingsomgeving, het risico-inschattingsproces en het proces voor monitoring, en met name die niet door het management worden aangepakt.
- Afwijkingen in het verleden, een verleden van fouten of een significant aantal correcties aan het einde van de verslagperiode.

Bijlage 3

(Zie par. 12(m), 21-26, A90-A181)

Inzicht in het systeem van interne beheersing van de entiteit

1. Het interne beheersingssysteem van de entiteit kan worden weerspiegeld in handboeken over beleidslijnen en procedures, systemen en formulieren, en de daarin ingebedde informatie, en wordt door mensen beïnvloed. Het systeem van interne beheersing van de entiteit wordt geïmplementeerd door het management, de met governance belaste personen en ander personeel op basis van de structuur van de entiteit. Het systeem van interne beheersing van de entiteit kan worden toegepast op basis van de beslissingen van het management, de met governance belaste personen of ander personeel en in de context van vereisten op grond van wet- en regelgeving, voor het operationele model van de entiteit, de juridische structuur van de entiteit, of een combinatie hiervan.

2. In deze bijlage worden de componenten van, evenals de beperkingen van, het systeem interne beheersing van de entiteit nader toegelicht zoals uiteengezet in paragrafen 12(m), 21-26 en A90-A181, aangezien deze betrekking hebben op een controle van financiële overzichten.

3. In het interne beheersingssysteem van de entiteit zijn aspecten opgenomen die betrekking hebben op de verslaggevingsdoelstellingen van de entiteit, inclusief de doelstellingen voor financiële verslaggeving, maar het kan ook aspecten omvatten die betrekking hebben op de doelstellingen op het gebied van de activiteiten of naleving van wet- en regelgeving, wanneer dergelijke aspecten relevant zijn voor financiële verslaggeving.

Voorbeeld:
Interne beheersingsmaatregelen over de naleving van wet- en regelgeving kunnen relevant zijn voor financiële verslaggeving wanneer dergelijke interne beheersingsmaatregelen relevant zijn voor het

opstellen door de entiteit van toelichtingen van voorwaardelijke gebeurtenissen in de financiële overzichten.

Componenten van het interne beheersingssysteem van de entiteit

Interne beheersingsomgeving

4. De interne beheersingsomgeving omvat de governance- en managementfuncties en de houding, bewustzijn en handelingen van de met governance belaste personen en het management met betrekking tot het systeem van interne beheersing van de entiteit, en het belang ervan in de entiteit. De interne beheersingsomgeving zet de toon van een organisatie, beïnvloedt het bewustzijn van de interne beheersing van zijn mensen en zorgt voor een algemene basis voor de werking van de andere componenten van het interne beheersingssysteem van de entiteit.

5. Het bewustzijn van de interne beheersing van een entiteit wordt beïnvloed door de met governance belaste personen, omdat een van hun rollen eruit bestaat om een tegenwicht te vormen tegen de druk op het management met betrekking tot de financiële verslaggeving die kan voortkomen uit marktverwachtingen of beloningsregelingen. De effectiviteit van de opzet van de interne beheersingsomgeving in relatie tot de betrokkenheid van de met governance belaste personen wordt daarom beïnvloed door aangelegenheden als:

   - Hun onafhankelijkheid van het management en hun bekwaamheid om de handelingen van management te evalueren.
   - Of ze inzicht hebben in de zakelijke transacties van de entiteit.
   - De mate waarin zij evalueren of de financiële overzichten zijn opgesteld in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving, inclusief of de financiële overzichten adequate toelichtingen bevatten.

6. De interne beheersingsomgeving omvat de volgende elementen:

   (a) *Hoe de verantwoordelijkheden van het management worden uitgevoerd, zoals het creëren en onderhouden van de cultuur van de entiteit en het tonen van de toewijding van het management aan integriteit en ethische waarden*. De effectiviteit van interne beheersingsmaatregelen kan niet boven de integriteit en ethische waarden van de mensen uitstijgen die ze creëren, uitvoeren en monitoren. Integriteit en ethisch gedrag zijn het product van de ethische en gedragsnormen of gedragscodes van de entiteit, hoe deze worden gecommuniceerd (bijvoorbeeld via uiteenzettingen over het beleid) en hoe deze in de praktijk worden versterkt (bijvoorbeeld via handelingen van het management om stimulansen of verleidingen die werknemers tot oneerlijke, onwettige of onethische handelingen zouden kunnen aanzetten, te elimineren of te verminderen). De communicatie van het beleid van de entiteit inzake integriteit en ethische waarden kan de communicatie van gedragsnormen aan personeel omvatten via uiteenzettingen van het beleid en gedragscodes en door het goede voorbeeld te geven.
   (b) *Wanneer de met governance belaste personen gescheiden zijn van het management, hoe de met governance belaste personen onafhankelijkheid van het management aantonen en toezicht uitoefenen op het interne beheersingssysteem van de entiteit*. Het bewustzijn van de interne beheersing van een entiteit wordt beïnvloed door de met governance belaste personen. Overwegingen kunnen omvatten of er voldoende personen zijn die onafhankelijk zijn van management en die objectief zijn in hun evaluaties en besluitvorming; hoe de met governance belaste personen de verantwoordelijkheden voor het toezicht identificeren en aanvaarden en of de met governance belaste personen verantwoordelijkheid behouden

voor toezicht op de opzet, implementatie en uitvoering door het management van het interne beheersingssysteem van de entiteit. Het belang van de verantwoordelijkheden van de met governance belaste personen wordt erkend in praktijkcodes en andere wet- en regelgeving of leidraden opgesteld ten behoeve van de met goverance belaste personen. Andere verantwoordelijkheden van de met governance belaste personen omvatten toezicht op de opzet en effectieve werking van klokkenluidersprocedures.

(c) *Hoe de entiteit autoriteit en verantwoordelijkheid toekent bij het nastreven van haar doelstellingen*. Dit kan overwegingen omvatten over:

- Belangrijke bevoegdheids- en verantwoordelijkheidsgebieden en geschikte rapportagelijnen;
- Beleidslijnen met betrekking tot passende handelspraktijken, kennis en ervaring van personeel op sleutelposities en middelen die voor het uitvoeren van taken beschikbaar worden gesteld; en
- Beleidslijnen en communicatie gericht op het waarborgen dat al het personeel de doelstellingen van de entiteit begrijpt, weet hoe hun individuele handelingen samenhangen en bijdraagt aan die doelstellingen, en herkent hoe en waarvoor ze verantwoordelijk worden gehouden.

(d) *Hoe de entiteit competente personen aantrekt, ontwikkelt en behoudt in overeenstemming met haar doelstellingen*. Dit omvat hoe de entiteit ervoor zorgt dat de personen de noodzakelijk kennis en vaardigheden hebben om de taken uit te voeren die het werk van de persoon definiëren, zoals:

- Normen voor het werven van de meest gekwalificeerde personen - met de nadruk op opleiding, eerdere werkervaring, prestaties uit het verleden en informatie over integriteit en ethisch gedrag.
- Trainingsbeleidslijnen die toekomstige rollen en verantwoordelijkheden communiceren, inclusief praktijken zoals opleidingsscholen en seminars die de verwachte niveaus van prestaties en gedrag aangeven; en
- Periodieke functioneringsgesprekken die promoties stimuleren die de toewijding van de entiteit voor de bevordering van gekwalificeerd personeel naar hogere verantwoordelijkheidsniveaus aantonen.

(e) *Hoe de entiteit personen verantwoording laat afleggen over hun verantwoordelijkheden bij het nastreven van de doelstellingen van het interne beheersingssysteem van de entiteit.* Dit kan bijvoorbeeld worden bereikt door:

- Mechanismen om te communiceren en personen verantwoordelijk te houden voor de uitvoering van verantwoordelijkheden inzake interne beheersing en corrigerende maatregelen te implementeren indien nodig;
- Prestatiemaatstaven, stimulansen en beloningen vast te stellen voor degenen die verantwoordelijk zijn voor het systeem van interne beheersing van de entiteit, inclusief hoe de maatregelen worden geëvalueerd en hun relevantie behouden;
- Hoe druk geassocieerd met het behalen van interne beheersingsdoelstellingen invloed heeft op de verantwoordelijkheden en prestatiemaatstaven van de personen; en
- Hoe de personen zo nodig worden gedisciplineerd.

De geschiktheid van bovenstaande aangelegenheden zal voor elke entiteit verschillen, afhankelijk van de grootte, de complexiteit van haar structuur en de aard van haar activiteiten.

Het risico-inschattingsproces van de entiteit

7. Het risico-inschattingsproces van de entiteit is een iteratief proces voor het identificeren en analyseren van risico's voor het bereiken van de doelstellingen van de entiteit en vormt de basis voor hoe het management of de met governance belaste personen de te beheersen risico's bepaalt.

8. Voor financiële verslaggevingsdoeleinden omvat het risico-inschattingsproces van de entiteit hoe het management bedrijfsrisico's identificeert die relevant zijn voor het opstellen van de financiële overzichten in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving van de entiteit, hun significantie inschat, de waarschijnlijkheid van hun voorkomen inschat, en beslist over handelingen om ze te beheersen en de resultaten daarvan. Het risico-inschattingsproces van de entiteit kan bijvoorbeeld ingaan op hoe de entiteit de mogelijkheid van niet-geregistreerde transacties overweegt of significante schattingen die zijn vastgelegd in de financiële overzichten identificeert en analyseert.

9. Risico's die relevant zijn voor betrouwbare financiële verslaggeving omvatten externe en interne gebeurtenissen, transacties of omstandigheden die kunnen voorkomen en die een negatieve invloed hebben op de mogelijkheid van een entiteit om financiële informatie te initiëren, vast te leggen, te verwerken en te rapporteren die consistent is met de beweringen van het management in de financiële overzichten. Het management kan plannen, programma's of handelingen initiëren om in te spelen op specifieke risico's of kan besluiten om een risico te nemen vanwege kosten of andere overwegingen. Risico's kunnen ontstaan of veranderen als gevolg van omstandigheden zoals de volgende:
    - *Veranderingen in de operationele omgeving*. Veranderingen in de regelgeving, economische of operationele omgeving kan leiden tot veranderingen in de concurrentiedruk en significante veranderingen in de risico's.
    - *Nieuw personeel*. Nieuw personeel kan een andere focus op of begrip van het systeem van interne beheersing van de entiteit hebben.
    - *Nieuw of vernieuwd informatiesysteem*. Significante en snelle veranderingen in het informatiesysteem kunnen het risico met betrekking tot het interne beheersingssysteem van de entiteit veranderen.
    - *Snelle groei*. Significante en snelle uitbreiding van de activiteiten kunnen de interne beheersingsmaatregelen onder druk zetten en het risico op falen van de interne beheersingsmaatregelen doen toenemen.
    - *Nieuwe technologie*. De invoering van nieuwe technologieën in productieprocessen of het informatiesysteem kan het risico met betrekking tot het interne beheersingssysteem van de entiteit veranderen.
    - *Nieuwe bedrijfsmodellen, producten of activiteiten*. Het ondernemen van activiteiten of het aangaan van transacties waarmee een entiteit weinig ervaring heeft, kan leiden tot nieuwe risico's met betrekking tot de interne beheersing.
    - *Reorganisaties*. Reorganisaties kunnen gepaard gaan met personeelsvermindering en wijzigingen in toezicht en functiescheiding die het risico met betrekking tot het systeem van interne beheersing van de entiteit kunnen veranderen.
    - *Uitbreiding van activiteiten in het buitenland*. De uitbreiding of overname van buitenlandse activiteiten brengt nieuwe en vaak unieke risico's met zich mee die van invloed kunnen zijn op de interne beheersing, bijvoorbeeld aanvullende of gewijzigde risico's op transacties in vreemde valuta.
    - *Nieuwe verslaggevingsregels*. De toepassing van nieuwe verslaggevingsprincipes of wijzigingen daarin kunnen van invloed zijn op risico's bij het opstellen van de financiële overzichten.

- *Gebruik van IT*. Risico's met betrekking tot:

    - Handhaving van de integriteit van gegevens en informatieverwerking;
    - Risico's voor de bedrijfsstrategie van de entiteit die zich voordoen als de IT-strategie van de entiteit niet effectief de bedrijfsstrategie van de entiteit ondersteunt; of
    - Veranderingen of onderbrekingen in de IT-omgeving van de entiteit of verloop van IT-personeel of wanneer de entiteit geen noodzakelijke updates aan de IT-omgeving uitvoert of dergelijke updates niet op tijd uitvoert.

Het proces van de entiteit om het systeem van interne beheersing te monitoren

10. Het proces van de entiteit om het systeem van interne beheersing te monitoren is een continu proces om de effectiviteit van het interne beheersingssysteem van de entiteit te evalueren en om noodzakelijke corrigerende maatregelen tijdig te nemen. Het proces van de entiteit om het interne beheersingssysteem van de entiteit te monitoren kan bestaan uit doorlopende activiteiten, afzonderlijke evaluaties (periodiek uitgevoerd) of een combinatie van beide. Doorlopende monitoringactiviteiten zijn vaak in de normale terugkerende activiteiten van een entiteit geïntegreerd en kunnen reguliere management- en toezichthoudende activiteiten omvatten. Het proces van de entiteit zal waarschijnlijk variëren in reikwijdte en frequentie afhankelijk van de inschatting van de risico's door de entiteit.

11. De doelstellingen en reikwijdte van interne auditfuncties omvatten doorgaans activiteiten die zijn opgezet om de effectiviteit van het interne beheersingssysteem van de entiteit te evalueren of te monitoren.[1] Het proces van de entiteit om het systeem van interne beheersing van de entiteit te monitoren kan activiteiten omvatten zoals de beoordeling door het management of aansluitingen van banksaldi tijdig worden opgesteld, dat interne auditors evalueren of de verkoopmedewerkers het beleid van de entiteit met betrekking tot de voorwaarden van verkoopcontracten naleven en dat een juridische afdeling toeziet op de naleving van de beleidslijnen van de entiteit inzake ethische of handelspraktijken. Monitoring moet er ook voor zorgen dat de interne beheersingsmaatregelen effectief blijven werken in de loop van de tijd. Bijvoorbeeld als de tijdigheid en de nauwkeurigheid van aansluitingen van banksaldi niet wordt gemonitord, zal het personeel waarschijnlijk stoppen met het opstellen hiervan.

12. Interne beheersingsmaatregelen met betrekking tot het proces van de entiteit om het systeem van interne beheersing van de entiteit te monitoren, inclusief die welke onderliggende geautomatiseerde interne beheersingsmaatregelen monitoren, kunnen geautomatiseerd of handmatig zijn, of een combinatie van beide. Een entiteit kan bijvoorbeeld geautomatiseerde interne beheersingsmaatregelen voor monitoring gebruiken voor de toegang tot bepaalde technologie met geautomatiseerde rapportages van ongebruikelijke activiteiten aan het management, dat handmatig geïdentificeerde afwijkingen onderzoekt.

13. Wanneer onderscheid wordt gemaakt tussen een monitoringactiviteit en een interne beheersingsmaatregel met betrekking tot het informatiesysteem, worden de onderliggende details van de activiteit in overweging genomen, vooral wanneer de activiteit een bepaald niveau van beoordeling door een leidinggevende omvat. Beoordelingen door een leidinggevende worden niet automatisch geclassificeerd als monitoringactiviteiten en het kan een kwestie van oordeelsvorming zijn of een beoordeling is geclassificeerd als een interne beheersingsmaatregel met betrekking tot het informatiesysteem of een monitoringactiviteit. Bijvoorbeeld de bedoeling van een maandelijkse interne beheersingsmaatregel op volledigheid zou zijn om fouten te

[1] ISA 610 en Bijlage 4 van deze ISA bieden verdere leidraden met betrekking tot interne audit.

detecteren en te corrigeren, waarbij een monitoringactiviteit zou vragen waarom fouten optreden en het management de verantwoordelijkheid toewijzen om het proces te repareren om toekomstige fouten te voorkomen. In eenvoudige termen, een interne beheersingsmaatregel met betrekking tot het informatiesysteem speelt in op een specifiek risico, terwijl een monitoringactiviteit inschat of interne beheersingsmaatregelen binnen elk van de vijf componenten van het interne systeem van de entiteit werken zoals bedoeld.

14. Monitoringactiviteiten kunnen het gebruik van informatie uit mededelingen van externe partijen omvatten die op problemen kunnen wijzen of de aandacht vestigen op gebieden die moeten worden verbeterd. Klanten bevestigen impliciet factureringsgegevens door hun facturen te betalen of te klagen over de in rekening gebrachte bedragen. Bovendien kunnen regelgevers of toezichthouders met de entiteit aangelegenheden bespreken die de werking van het systeem interne beheersing van de entiteit beïnvloeden, bijvoorbeeld mededelingen met betrekking tot onderzoeken door regelgevende of toezichthoudende instanties voor de banksector. Ook kan het management bij het uitvoeren van monitoringactiviteiten rekening houden met mededelingen door auditors met betrekking tot het systeem van interne beheersing van de entiteit.

Het informatiesysteem en de communicatie

15. Het informatiesysteem dat relevant is voor het opstellen van de financiële overzichten bestaat uit activiteiten en beleidslijnen en administratieve en ondersteunende vastleggingen, opgezet en ingericht om:

- Transacties van de entiteit te initiëren, registreren en verwerken (evenals vastleggen, verwerken en toelichten van informatie over andere gebeurtenissen en omstandigheden dan transacties) en om verantwoording af te leggen voor de daarmee verband houdende activa, passiva en eigen vermogen;
- Onjuiste verwerking van transacties op te lossen, bijvoorbeeld geautomatiseerde tussenrekeningen en procedures die worden gevolgd om elementen op deze tussenrekeningen tijdig uit te zoeken;
- Het doorbreken van het systeem of het omzeilen van interne beheersingsmaatregelen te verwerken en te verantwoorden;
- Informatie van transactieverwerking opnemen in het grootboek (bijv. overdracht van geaccumuleerde transacties uit een subgrootboek);
- Informatie verzamelen en verwerken die relevant is voor het opstellen van de financiële overzichten voor andere gebeurtenissen en omstandigheden dan transacties, zoals de afschrijving van activa en veranderingen in de invorderbaarheid van activa; en
- Ervoor te zorgen dat informatie die moet worden toegelicht in het van toepassing zijnde stelsel inzake financiële verslaggeving, wordt verzameld, vastgelegd, verwerkt, samengevat en op passende wijze gerapporteerd in de financiële overzichten.

16. De bedrijfsprocessen van een entiteit omvatten de activiteiten die zijn opgezet om:

- De producten en diensten van een entiteit te ontwikkelen, kopen, produceren, verkopen en distribueren;
- Te zorgen voor naleving van wet- en regelgeving; en
- Informatie vast te leggen, inclusief boekhoudkundige en financiële verslaggevingsinformatie.

Bedrijfsprocessen resulteren in de transacties die worden geregistreerd, verwerkt en gerapporteerd door het informatiesysteem.

17. De kwaliteit van informatie is van invloed op de mogelijkheid van het management om juiste beslissingen te nemen bij het leiden en beheersen van de activiteiten van de entiteit en om betrouwbare financiële verslagen op te stellen.

18. Communicatie, waarbij inzicht wordt verkregen in individuele rollen en verantwoordelijkheden met betrekking tot het systeem van interne beheersing van de entiteit, kan de vorm aannemen van handboeken over beleidslijnen, administratieve verwerking en financiële verslaggeving en memoranda. Communicatie kan ook elektronisch, mondeling en door de handelingen van het management plaatsvinden.

19. Communicatie door de entiteit van de financiële verslaggevingsrollen en -verantwoordelijkheden en van significante aangelegenheden met betrekking tot financiële verslaggeving omvat het verschaffen van inzicht in individuele rollen en verantwoordelijkheden met betrekking tot het systeem van interne beheersing van de entiteit dat relevant is voor financiële verslaggeving. Het kan aangelegenheden omvatten als de mate waarin het personeel begrijpt hoe hun activiteiten in het informatiesysteem betrekking hebben op het werk van anderen en de middelen om uitzonderingen op een passend hoger niveau binnen de entiteit te rapporteren.

Interne beheersingsactiviteiten

20. Interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten"" worden geïdentificeerd in overeenstemming met paragraaf 26. Dergelijk interne beheersingsmaatregelen omvatten interne beheersingsmaatregelen voor informatieverwerking en *general IT controls*, beide kunnen handmatig of geautomatiseerd van aard zijn. Hoe groter de mate van geautomatiseerde interne beheersingsmaatregelen, of interne beheersingsmaatregelen met geautomatiseerde aspecten, die het management gebruikt en waarop het steunt met betrekking tot haar financiële verslaggeving, hoe belangrijker het voor de entiteit kan worden om *general IT controls* te implementeren die de voortdurende werking van de geautomatiseerde aspecten van interne beheersingsmaatregelen voor informatieverwerking behandelen. Interne beheersingsmaatregelen in de component "interne beheersingsactiviteiten" kunnen betrekking hebben op:

    - *Autorisatie en goedkeuringen*. Een autorisatie bevestigt dat een transactie geldig is (d.w.z. vertegenwoordigt een feitelijke economische gebeurtenis of valt binnen de beleidslijnen van een entiteit). Meestal neemt een autorisatie de vorm aan van een goedkeuring door een hoger managementniveau of van verificatie en een bepaling of de transactie geldig is. Een leidinggevende keurt bijvoorbeeld een onkostendeclaratie goed na beoordeling of de kosten redelijk en binnen de beleidslijnen lijken. Een voorbeeld van een geautomatiseerde goedkeuring is wanneer de kosten per eenheid op de factuur automatisch worden vergeleken met de gerelateerde kosten per eenheid op de inkooporder binnen een vooraf vastgesteld tolerantieniveau. Facturen binnen het tolerantie niveau worden automatisch goedgekeurd voor betaling. Die facturen buiten het tolerantieniveau zijn gemarkeerd voor aanvullend onderzoek.
    - *Aansluitingen*- Aansluitingen vergelijken twee of meer gegevenselementen. Als verschillen zijn geïdentificeerd, wordt actie ondernomen om de gegevens in overeenstemming te brengen. Aansluitingen hebben meestal betrekking op de volledigheid of nauwkeurigheid van de verwerking van transacties.
    - *Verificaties*- Verificaties vergelijken twee of meer elementen met elkaar of vergelijken een element met een beleidslijn, en zullen waarschijnlijk een vervolgactie inhouden wanneer de twee elementen niet overeenkomen of het element niet in overeenstemming is met

beleidslijnen. Verificaties hebben meestal betrekking op de volledigheid, nauwkeurigheid, of geldigheid van verwerking van transacties.

- *Fysieke of logische interne beheersingsmaatregelen, inclusief die waarmee de beveiliging van activa tegen ongeautoriseerde toegang, verwerving, gebruik of verwijdering wordt behandeld*. Deze interne beheersingsmaatregelen omvatten:

  - De fysieke beveiliging van activa, inclusief adequate waarborgen zoals beveiligde faciliteiten over toegang tot activa en vastleggingen.
  - De autorisatie voor toegang tot computerprogramma's en gegevensbestanden (d.w.z. logische toegang).
  - De periodieke tellingen en vergelijkingen met bedragen in controlebestanden (bijvoorbeeld het vergelijken van de resultaten van tellingen van contant geld, effecten en voorraden met de administratieve vastleggingen).

  De mate waarin fysieke interne beheersingsmaatregelen ter voorkoming van diefstal van activa relevant zijn voor de betrouwbaarheid van de opstelling van de financiële overzichten hangt af van omstandigheden zoals wanneer activa zijn zeer vatbaar voor oneigenlijke toe-eigening.

- *Functiescheiding*. De toewijzing aan verschillende personen van de verantwoordelijkheden voor het autoriseren van transacties, het vastleggen van transacties en het bewaren van activa . Functiescheiding is bedoeld om beperkingen aan te brengen in de mogelijkheden voor wie dan ook om bij de uitoefening van zijn normale taken fouten te maken en te verhullen of fraude te plegen en te verhullen.

  Een manager die kredietverkopen autoriseert, is bijvoorbeeld niet verantwoordelijk voor het bijhouden van debiteurenrekeningen of afhandeling van contante betalingen. Als één persoon al deze activiteiten kan uitvoeren, zou de persoon bijvoorbeeld een fictieve verkoop kunnen creëren die onopgemerkt kan blijven. Evenzo mogen verkopers niet in staat zijn productprijsbestanden of commissietarieven te wijzigen.

  Soms is scheiding niet praktisch uitvoerbaar, kosteneffectief of haalbaar. Kleinere en minder complexe entiteiten kunnen wellicht voldoende middelen missen om een ideale scheiding te bereiken en de kosten van het inhuren van extra personeel kunnen belemmerend zijn. In deze situaties kan het management alternatieve interne beheersingsmaatregelen instellen. Als in het bovenstaande voorbeeld de verkoper productprijsbestanden kan wijzigen, kan een detecterende interne beheersingsmaatregel worden ingesteld om personeel dat niet betrokken is bij de verkoopfunctie periodiek te laten beoordelen of en onder welke omstandigheden de verkoper de prijzen heeft gewijzigd.

21. Bepaalde interne beheersingsmaatregelen kunnen afhankelijk zijn van het bestaan van passende toezichthoudende interne beheersingsmaatregelen die zijn vastgesteld door het management of de met governance belaste personen. Autorisatiecontroles kunnen bijvoorbeeld zijn gedelegeerd volgens vastgestelde richtlijnen, zoals investeringscriteria die door de met governance belaste personen zijn vastgesteld; anderzijds kunnen niet-routinematige transacties zoals significante overnames of desinvesteringen specifieke goedkeuring op hoog niveau vereisen, waaronder in sommige gevallen die van aandeelhouders.

Beperkingen van interne beheersing

22. Hoe effectief het interne beheersingssysteem van een entiteit ook is, het kan een entiteit slechts een redelijke mate van zekerheid verschaffen over het behalen van de doelstellingen inzake financiële verslaggeving van de entiteit. De waarschijnlijkheid van het behalen ervan wordt beïnvloed door de inherente beperkingen van interne beheersing. Deze omvatten de realiteit dat mensen bij hun besluitvorming foutieve beoordelingen kunnen maken en dat verstoringen in het systeem van interne beheersing van de entiteit als gevolg van menselijke fouten kunnen voorkomen. Er kan bijvoorbeeld een fout optreden in de opzet of wijziging van een interne beheersingsmaatregel. Eveneens is het mogelijk dat een interne beheersingsmaatregel niet effectief werkt, bijvoorbeeld als informatie die wordt verzameld ten behoeve van het interne beheersingssysteem van de entiteit (bijvoorbeeld een uitzonderingsrapport) niet effectief wordt gebruikt omdat de persoon die verantwoordelijk is voor het beoordelen van de informatie het doel ervan niet begrijpt of nalaat passende maatregelen te nemen.

23. Bovendien kunnen interne beheersingsmaatregelen worden omzeild door samenspanning van twee of meer mensen of doordat het management op ongepaste wijze interne beheersingsmaatregelen doorbreekt. Het management kan bijvoorbeeld nevenovereenkomsten sluiten met klanten die de algemene bepalingen en voorwaarden van de standaardverkoopcontracten van de entiteit wijzigen, wat tot een onjuiste opbrengstverantwoording kan leiden. Ook kunnen de in een IT-applicatie geïntegreerde wijzigingscontroles die gericht zijn op het identificeren en rapporteren van transacties die gespecificeerde kredietlimieten overschrijden, worden doorbroken of uitgeschakeld.

24. Verder kan het management bij het opzetten en implementeren van interne beheersingsmaatregelen oordeelsvormingen maken over de aard en de omvang van de interne beheersingsmaatregelen die het wil implementeren en de aard en de omvang van de risico's die het wenst te aanvaarden.

Bijlage 4

(Zie par. 14(a), 24(a)(ii), A25-A28, A118)

Overwegingen voor het verwerven van inzicht in de interne auditfunctie van een entiteit

Deze bijlage geeft verdere overwegingen met betrekking tot het verwerven van inzicht in de interne auditfunctie van de entiteit wanneer een dergelijke functie bestaat.

Doelstellingen en reikwijdte van de interne auditfunctie

1. De doelstellingen en reikwijdte van een interne auditfunctie, de aard van haar verantwoordelijkheden en haar status binnen de organisatie, inclusief de bevoegdheid en verantwoordingsplicht van de functie, variëren in grote mate en zijn afhankelijk van de omvang, complexiteit en structuur van de entiteit en de vereisten van het management en, waar van toepassing, de met governance belaste personen. Deze aangelegenheden kunnen worden uiteengezet in een internal audit charter of taakomschrijving.

2. De verantwoordelijkheden van een interne auditfunctie kunnen het uitvoeren van werkzaamheden en de evaluatie van de resultaten hiervan omvatten om aan het management en aan de met governance belaste personen een bepaalde mate van zekerheid te verschaffen met betrekking tot de opzet en effectiviteit van risicobeheersing, het systeem van interne

beheersing en governance-processen van de entiteit. Wanneer dit het geval is, kan de interne auditfunctie een belangrijke rol spelen in het proces van monitoren van het systeem van interne beheersing van de entiteit. De verantwoordelijkheden van de interne auditfunctie kunnen echter zijn gericht op het evalueren van kostenefficiëntie, doelmatigheid en doeltreffendheid van activiteiten en, wanneer dit het geval is, kunnen de werkzaamheden van de functie niet direct gerelateerd zijn aan de financiële verslaggeving van de entiteit.

Verzoeken om inlichtingen bij de interne auditfunctie

3. Als een entiteit een interne auditfunctie heeft, kunnen verzoeken om inlichtingen bij de juiste personen binnen de functie informatie verschaffen die nuttig is voor de auditor bij het verwerven van inzicht in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving en het systeem van interne beheersing van de entiteit en bij het identificeren en inschatten van risico's op een afwijking van materieel belang op het niveau van de financiële overzichten en beweringen. Bij de uitvoering van haar werkzaamheden heeft de interne auditfunctie waarschijnlijk inzicht verkregen in de activiteiten en bedrijfsrisico's van de entiteit en kan bevindingen hebben op basis van haar werkzaamheden, zoals geïdentificeerde tekortkomingen in de interne beheersing of risico's, die een waardevolle *input* kunnen vormen voor het inzicht van de auditor in de entiteit en haar omgeving, het van toepassing zijnde stelsel inzake financiële verslaggeving, het systeem van interne beheersing van de entiteit, de risico-inschattingen van de auditor of andere aspecten van de controle. Verzoeken om inlichtingen van de auditor worden daarom gedaan ongeacht of de auditor verwacht gebruik te maken van het werk van de interne auditfunctie om de aard of timing van uit te voeren controlewerkzaamheden te wijzigen of de omvang daarvan te verminderen.[1] Verzoeken om inlichtingen die in het bijzonder relevant zijn, kunnen zowel aangelegenheden betreffen die de interne auditfunctie heeft besproken met de met governance belaste personen als de uitkomsten van het eigen risico-inschattingsproces van de interne auditfunctie.

4. Indien op basis van de reacties op de verzoeken om inlichtingen van de auditor blijkt dat er bevindingen zijn die relevant kunnen zijn voor de financiële verslaggeving van de entiteit en de voor de controle van de financiële overzichten, kan de auditor het als passend beschouwen om daaraan gerelateerde rapporten van de interne auditfunctie te lezen. Voorbeelden van rapportages van de interne auditfunctie die relevant kunnen zijn, omvatten de strategie- en planningsdocumenten van de functie en rapportages die zijn opgesteld voor het management of voor de met governance belaste personen, waarin de bevindingen van de onderzoeken van de interne auditfunctie zijn beschreven.

5. Bovendien, in overeenstemming met ISA 240,[2] als de interne auditfunctie informatie verschaft aan de auditor met betrekking tot feitelijke, vermoedelijke of vermeende fraude, houdt de auditor hier rekening mee bij het door de auditor identificeren van het risico op een afwijking van materieel belang als gevolg van fraude.

6. Juiste personen binnen de interne auditfunctie bij wie verzoeken om inlichtingen worden gedaan, zijn degenen die, naar het oordeel van de auditor, over passende kennis, ervaring en autoriteit beschikken, zoals de chief internal audit executive of, afhankelijk van de omstandigheden, overige medewerkers binnen de functie. De auditor kan het ook passend achten om met deze personen periodiek overleg te plegen.

---

[1] De relevante vereisten zijn opgenomen in ISA 610 (herzien 2013).

[2] ISA 240, paragraaf 19.

Overweging van de interne auditfunctie bij het verwerven van inzicht in de interne beheersingsomgeving

7. Bij het verwerven van inzicht in de interne beheersingsomgeving kan de auditor overwegen hoe het management heeft gereageerd op de bevindingen en aanbevelingen van de interne auditfunctie met betrekking tot geïdentificeerde tekortkomingen in de interne beheersing die relevant zijn voor het opstellen van de financiële overzichten, inclusief of en hoe dergelijke reacties zijn geïmplementeerd en of ze vervolgens zijn geëvalueerd door de interne audit functie.

Inzicht in de rol die de interne auditfunctie speelt in proces van de entiteit om het systeem van interne beheersing te monitoren

8. Indien de aard van de verantwoordelijkheden en van de assurance-activiteiten van de interne auditfunctie verband houden met de financiële verslaggeving van de entiteit, kan de auditor tevens gebruikmaken van de werkzaamheden van de interne auditfunctie om de aard of timing van controlewerkzaamheden die door de auditor zelf worden uitgevoerd bij het verkrijgen van controle-informatie aan te passen, of de omvang hiervan te verminderen. Het is waarschijnlijker dat auditors in staat zullen zijn om gebruik te maken van het werk van een interne auditfunctie van de entiteit wanneer bijvoorbeeld blijkt dat, op basis van ervaring in voorgaande controles of de risico-inschattingswerkzaamheden van de auditor, de entiteit over een interne auditfunctie beschikt die n adequate en gepaste middelen heeft die in verhouding staan tot de complexiteit van de entiteit en de aard van haar activiteiten en die een directe rapportagelijn heeft met de met governance belaste personen.

9. Indien op basis van het voorlopige inzicht van de auditor in de interne auditfunctie, de auditor verwacht om gebruik te maken van de werkzaamheden van de interne auditfunctie om de aard of timing van de uit te voeren controlewerkzaamheden te wijzigen of om de omvang daarvan te verminderen, is ISA 610 van toepassing.

10. Zoals verder in ISA 610 wordt besproken, verschillen de werkzaamheden van een interne auditfunctie van andere op monitoring gerichte interne beheersingsmaatregelen die relevant kunnen zijn voor de financiële verslaggeving, zoals de beoordelingen van management accounting informatie die zijn opgezet om bij te dragen aan de manier waarop de entiteit afwijkingen voorkomt of detecteert.

11. Het vroegtijdig in de opdracht tot stand brengen van communicatie met de juiste personen binnen de interne auditfunctie van een entiteit en het onderhouden van dergelijke communicatie gedurende de opdracht, kan het effectief delen van informatie bevorderen. Het creëert een omgeving waarin de auditor kan worden geïnformeerd over significante aangelegenheden die onder de aandacht van de interne auditfunctie kunnen komen wanneer dergelijke aangelegenheden de werkzaamheden van de auditor kunnen beïnvloeden. 200 behandelt het belang van de auditor om de controle te plannen en uit te voeren met een professioneel-kritische instelling,[3] inclusief alert zijn op informatie die de betrouwbaarheid van documenten en reacties op verzoeken om inlichtingen die als controle-informatie worden gebruikt, ter discussie stelt. Dienovereenkomstig kan overleg met de interne auditfunctie gedurende de opdracht aan de interne auditors de gelegenheid bieden om dergelijke informatie onder de aandacht van de auditor te brengen. De auditor is dan in staat om dergelijke informatie in overweging te nemen bij de identificatie en inschatting van risico's op een afwijking van materieel belang door de auditor.

[3] ISA 200, paragraaf 7.

Bijlage 5
(Zie par. 25(a), 26(b)-(c), A94, A166-A172)

Overwegingen voor het verwerven van inzicht in informatietechnologie (IT)

Deze bijlage geeft verdere aangelegenheden die de auditor kan overwegen bij het verwerven van inzicht in het gebruik van IT door de entiteit in haar systeem van interne beheersing.

Inzicht in het gebruik van informatietechnologie door de entiteit in de componenten van het systeem van interne beheersing van de entiteit

1. Het interne beheersingssysteem van een entiteit bevat handmatige elementen en geautomatiseerde elementen (dat wil zeggen, handmatige en geautomatiseerde interne beheersingsmaatregelen en andere middelen die worden gebruikt in het interne beheersingssysteem van de entiteit). De combinatie van handmatige en geautomatiseerde elementen in een entiteit is afhankelijk van de aard en complexiteit van het gebruik van IT door de entiteit. Het gebruik van IT door een entiteit beïnvloedt de manier waarop de informatie die relevant is voor het opstellen van de financiële overzichten in overeenstemming met het van toepassing zijnde stelsel inzake financiële verslaggeving, wordt verwerkt, opgeslagen en gecommuniceerd en beïnvloedt daarom de manier waarop het interne beheersingssysteem van de entiteit is opgezet en geïmplementeerd. Elke component van het interne beheersingssysteem van de entiteit kan een zekere mate van IT gebruiken.

   Over het algemeen komt IT het interne beheersingssysteem van een entiteit ten goede omdat het een entiteit in staat stelt om:

   - Vooraf gedefinieerde bedrijfsregels consistent toe te passen en complexe berekeningen uit te voeren bij de verwerking van grote hoeveelheden transacties of gegevens;
   - De tijdigheid, beschikbaarheid en nauwkeurigheid van informatie te verbeteren;
   - Aanvullende analyse van informatie te vergemakkelijken;
   - De uitvoering van haar activiteiten en haar beleidslijnen en procedures beter te monitoren;
   - Het risico te beperken dat interne beheersingsmaatregelen worden omzeild; en
   - De mogelijkheid te verbeteren om effectieve functiescheiding te bereiken door beveiligingsmaatregelen te implementeren in IT-applicaties, databases en besturingssystemen.

2. De kenmerken van handmatige of geautomatiseerde elementen zijn relevant voor de identificatie en inschatting van de risico's op een afwijking van materieel belang door de auditor en verdere daarop gebaseerde controlewerkzaamheden. Geautomatiseerde interne beheersingsmaatregelen kunnen betrouwbaarder zijn dan handmatige interne beheersingsmaatregelen omdat ze niet zo gemakkelijk kunnen worden omzeild, genegeerd of doorbroken en ze zijn ook minder gevoelig voor eenvoudige fouten en vergissingen. Geautomatiseerde interne beheersingsmaatregelen kunnen in de volgende omstandigheden effectiever zijn dan handmatige interne beheersingsmaatregelen:

   - Grote aantallen van terugkerende transacties, of in situaties waarin te voorziene of te voorspellen fouten kunnen worden voorkomen, of gedetecteerd en gecorrigeerd door automatisering.
   - Interne beheersingsmaatregelen waarbij de specifieke manieren voor de uitvoering daarvan adequaat kunnen worden opgezet en geautomatiseerd.

Inzicht in het gebruik van informatietechnologie door de entiteit in het informatiesysteem (Zie par. 25 (a))

3. Het informatiesysteem van de entiteit kan het gebruik van handmatige en geautomatiseerde elementen omvatten, die ook invloed hebben op de manier waarop transacties worden geïnitieerd, vastgelegd, verwerkt en gerapporteerd. Met name procedures voor het initiëren, registreren, verwerken en rapporteren van transacties kunnen via de IT applicaties gebruikt door de entiteit worden afgedwongen en de manier waarop de entiteit die applicaties heeft geconfigureerd. Daarnaast, kunnen vastleggingen in de vorm van digitale informatie vastleggingen in de vorm van papieren documenten vervangen of aanvullen.

4. Bij het verwerven van inzicht in de IT-omgeving die relevant is voor de transactiestromen en informatieverwerking in het informatiesysteem, verzamelt de auditor informatie over de aard en kenmerken van de gebruikte IT-applicaties, evenals de ondersteunende IT-infrastructuur en IT. De volgende tabel bevat voorbeelden van aangelegenheden die de auditor kan overwegen bij het verwerven van inzicht in de IT-omgeving en bevat voorbeelden van typische kenmerken van IT omgevingen op basis van de complexiteit van IT-applicaties die worden gebruikt in het informatiesysteem van de entiteit. Dergelijke kenmerken zijn echter richtinggevend en kunnen verschillen, afhankelijk van de aard van de specifieke IT-applicaties die door een entiteit worden gebruikt.

	Voorbeelden van typische kenmerken van:		
	Niet complexe commerciële software	**Middelgrote en redelijk complexe commerciële software of IT-applicaties**	**Grote of complexe IT-applicaties (bijvoorbeeld ERP systemen)**
Aangelegenheden die verband houden met de mate van automatisering en gebruik van gegevens:			
• De mate van geautomatiseerde procedures voor verwerking en de complexiteit van die procedures, inclusief of er sprake is van hoog geautomatiseerde, papierloze verwerking is.	N.V.T.	N.V.T.	Uitgebreide en vaak complexe geautomatiseerde procedures
• De mate van steunen op systeem gegenereerde rapporten door de entiteit in de verwerking van informatie	Eenvoudige geautomatiseerde rapport logica	Eenvoudige relevante geautomatiseerde rapport logica	Complexe geautomatiseerde rapport logica; rapport generator software
• Hoe gegevens worden ingevoerd (d.w.z. handmatige invoer, klant- of leveranciersinvoer of	Handmatige gegevensinvoer	Kleine aantallen gegevensinvoer of eenvoudige interfaces	Grote aantallengegevensinvoer of complexe interfaces

	Voorbeelden van typische kenmerken van:		
	Niet complexe commerciële software	**Middelgrote en redelijk complexe commerciële software of IT-applicaties**	**Grote of complexe IT-applicaties (bijvoorbeeld ERP systemen)**
het laden van bestanden).			
• Hoe IT communicatie tussen applicaties, databases of andere aspecten van de IT omgeving faciliteert, intern en extern, indien passend, door systeem interfaces.	Geen geautomatiseerde interfaces (alleen handmatige invoer)	Kleine aantallen gegevensinvoer of eenvoudige interfaces	Grote aantallen gegevensinvoer of complexe interfaces
• Het aantal en de complexiteit van gegevens in digitale vorm verwerkt door het informatiesysteem, inclusief of administratieve vastleggingen of andere informatie is opgeslagen in digitale vorm en de locatie van opgeslagen gegevens.	Kleine aantallen gegevens of eenvoudige gegevens die handmatig kunnen worden geverifieerd; Gegevens lokaal beschikbaar	Kleine aantallen gegevens of eenvoudige gegevens	Grote aantallen gegevens of complexe gegevens; Data warehouses;[1] Gebruik van interne of externe IT-service providers (bijv. opslag van derden of *hosting* van gegevens)
Aangelegenheden die verband houden met de IT applicaties en IT infrastructuur:			
• Het type applicatie(bijv. een commerciële toepassing met weinig of geen maatwerk, of een sterk aangepaste of in hoge mate geïntegreerde applicatie die mogelijk is gekocht en aangepast, of in eigen huis ontwikkeld).	Gekochte applicatie met weinig of geen maatwerk	Gekochte applicatie of eenvoudige verouderde of *low-end* ERP-applicaties met weinig of geen maatwerk	Op maat ontwikkelde applicaties of complexere ERP's met significant maatwerk
• De complexiteit van de aard van de IT applicaties en de onderliggende IT infrastructuur.	Kleine, eenvoudige laptop of client server	Volwassen en stabiel mainframe, kleine of	Complex mainframe, grote of complexe client server, web-gerichte,

[1] Een datawarehouse wordt over het algemeen beschreven als een centrale opslagplaats van geïntegreerde gegevens uit een of meer verschillende bronnen (zoals meerdere databases) waaruit rapporten kunnen worden gegenereerd of die door de entiteit kunnen worden gebruikt voor andere data analyse-activiteiten. Een rapportgenerator is een IT-applicatie die wordt gebruikt om gegevens te extraheren uit een of meer bronnen (zoals een datawarehouse, een database of een IT-applicatie) en die de gegevens presenteert in een gespecificeerd formaat.

	Voorbeelden van typische kenmerken van:		
	Niet complexe commerciële software	**Middelgrote en redelijk complexe commerciële software of IT-applicaties**	**Grote of complexe IT-applicaties (bijvoorbeeld ERP systemen)**
	gebaseerde oplossing	eenvoudige client server, software als een service cloud	infrastructuur als een service cloud
• Of er sprake is van *third party hosting* of uitbesteding van IT.	Indien uitbesteed, competente, volwassen, bewezen leverancier (bijv. cloud provider)	Indien uitbesteed, competente, volwassen, bewezen provider (bijv. cloud provider)	Competente, volwassen bewezen leverancier voor bepaalde applicaties en nieuwe of startup provider voor anderen
• Of de entiteit nieuwe technologieën gebruikt die invloed hebben op haar financiële verslaggeving.	Geen gebruik van nieuwe technologieën	Beperkt gebruik van nieuwe technologieën in sommige applicaties	Gemengd gebruik van nieuwe technologieën over platforms heen
Aangelegenheden gerelateerd aan IT processen:			
• Het personeel betrokken bij het onderhouden van de IT omgeving (het aantal en vaardigheidsniveau van de IT ondersteunende middelen die de beveiliging beheren en veranderingen in de IT omgeving).	Weinig personeel met beperkte IT-kennis om leveranciers upgrades te verwerken en toegang te beheren	Beperkt personeel met IT-vaardigheden / gewijd aan IT	Toegewijde IT afdelingen met bekwaam personeel, inclusief programmeervaardigheden
• De complexiteit van processen om toegangsrechten te beheren.	Een enkele persoon met beheerders toegang beheert toegangsrechten	Weinig personen met beheerderstoegang beheren toegangsrechten	Complexe processen beheerd door IT afdeling voor toegangsrechten
• De complexiteit van de beveiliging over de IT omgeving, inclusief kwetsbaarheid van de IT applicaties, databases, en andere aspecten van de IT omgeving voor cyberrisico's, vooral wanneer er web-	Eenvoudige toegang ter plaatse zonder externe web-gerichte elementen	Sommige web-gebaseerde applicaties met voornamelijk eenvoudige, rol-gebaseerde beveiliging	Meerdere platforms met web-gebaseerde toegang en complexe beveiligings-modellen

	Voorbeelden van typische kenmerken van:		
	Niet complexe commerciële software	**Middelgrote en redelijk complexe commerciële software of IT-applicaties**	**Grote of complexe IT-applicaties (bijvoorbeeld ERP systemen)**
gebaseerde transacties zijn of transacties waarbij externe interfaces betrokken zijn.			
• Of programma wijzigingen zijn gemaakt in de manier waarop informatie wordt verwerkt en de omvang van zulke veranderingen tijdens de verslagperiode.	Commerciële software zonder geïnstalleerde broncode	Enkele commerciële applicaties zonder broncode en andere volwassen applicaties met een klein aantal of eenvoudige veranderingen; traditionele levenscyclus van systeemontwikkeling	Nieuw of groot aantal of complexe veranderingen, verschillende ontwikkelingscycli elk jaar.
• De mate van wijziging binnen de IT-omgeving (bijvoorbeeld nieuwe aspecten van de IT-omgeving of significante wijzigingen in de IT-applicaties of de onderliggende IT infrastructuur).	Wijzigingen beperkt tot versie-upgrades van commerciële software	Wijzigingen bestaan uit commerciële software upgrades, ERP versie-upgrades, of verbeteringen aan verouderde systemen	Nieuwe, groot aantal of complexe veranderingen, verschillende ontwikkelingscycli elk jaar, forse ERP-aanpassing
• Of er een significante dataconversie was tijdens de verslagperiode en, indien dit het geval is, de aard en significantie van de aangebrachte wijzigingen en hoe de conversie was ondernomen.	Software-upgrades geleverd door de leverancier; Geen gegevensconversie kenmerken voor upgrade	Kleine versie upgrades voor commerciële software applicaties met beperkte gegevens conversie	Aanzienlijke versie upgrade, nieuwe release, platform verandering

Nieuwe technologieën

5. Entiteiten kunnen nieuwe technologieën gebruiken (bijv. blockchain, robotica of kunstmatige intelligentie) omdat dergelijke technologieën specifieke kansen kunnen bieden om de operationele efficiëntie te verhogen of de financiële verslaggeving te verbeteren. Wanneer nieuwe technologieën gebruikt worden in het informatiesysteem van de entiteit dat relevant is bij het opstellen van de financiële overzichten, kan de auditor dergelijke technologieën opnemen in de

identificatie van IT-applicaties en andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT. Terwijl nieuwe technologieën wellicht als geavanceerder of complexer worden beschouwd in vergelijking met bestaande technologieën, blijven de verantwoordelijkheden van de auditor met betrekking tot IT-applicaties en geïdentificeerde *general IT controls* in overeenstemming met paragraaf 26 (b) - (c) ongewijzigd.

Schaalbaarheid

6. Het verwerven van inzicht in de IT-omgeving van de entiteit kan gemakkelijker worden bereikt voor een minder complexe entiteit die commerciële software gebruikt en wanneer de entiteit geen toegang heeft tot de broncode om programmawijzigingen aan te brengen. Dergelijke entiteiten hebben misschien geen specifieke IT-middelen, maar kan een persoon toegewezen hebben in een beheerdersrol met als doel het verlenen van toegang voor werknemers of installeren van door de leverancier geleverde updates voor de IT-applicaties. Specifieke aangelegenheden die de auditor kan overwegen om inzicht te verwerven in de aard van een commercieel boekhoudsoftwarepakket n wat de enige IT-applicatie kan zijn die door een minder complexe entiteit in zijn informatiesysteem wordt gebruikt, kunnen omvatten:

    - De mate waarin de software gevestigd is en een reputatie van betrouwbaarheid heeft;
    - De mate waarin het voor de entiteit mogelijk is om de broncode van de software te wijzigen om extra modules (bijv. *add-ons*) toe te voegen aan de basissoftware, of om directe wijzigingen aan gegevens aan te brengen;
    - De aard en omvang van wijzigingen die in de software zijn aangebracht. Hoewel een entiteit mogelijk niet in staat is om de broncode van de software te wijzigen, laten veel softwarepakketten configuratie toe (bijvoorbeeld het instellen of wijzigen van rapportageparameters). Meestal gaat het hier niet om wijzigingen in de broncode; de auditor kan echter overwegen in hoeverre de entiteit de software kan configureren wanneer hij de volledigheid en nauwkeurigheid van informatie geproduceerd door de software die wordt gebruikt als controle-informatie beschouwt; en
    - De mate waarin gegevens met betrekking tot het opstellen van de financiële overzichten direct kunnen zijn benaderd (d.w.z. directe toegang tot de database zonder de IT-applicatie te gebruiken) en het aantal gegevens dat worden verwerkt. Hoe groter het aantal gegevens, hoe groter de kans dat de entiteit interne beheersingsmaatregelen nodig heeft die betrekking hebben op het handhaven van de integriteit van de gegevens, waaronder general IT-controls over ongeautoriseerde toegang en wijzigingen in de gegevens.

7. Complexe IT-omgevingen kunnen sterk aangepaste of in hoge mate geïntegreerde IT-applicaties omvatten en het kan daarom meer moeite vereisen om deze te begrijpen. Financiële verslaggevingsprocessen of IT-applicaties kunnen worden geïntegreerd met andere IT-applicaties. Een dergelijke integratie kan betrekking hebben op IT-applicaties die worden gebruikt in de bedrijfsactiviteiten van de entiteit en die informatie verstrekken aan de IT-applicaties die relevant zijn voor de transactiestromen en informatieverwerking in het informatiesysteem van de entiteit. In zulke omstandigheden kunnen bepaalde IT-applicaties die worden gebruikt in de bedrijfsactiviteiten van de entiteit ook relevant zijn bij het opstellen van de financiële overzichten. Complexe IT-omgevingen vereisen mogelijk ook specifieke IT-afdelingen met gestructureerde IT-processen, ondersteund door personeel dat vaardigheden heeft op het gebied van software ontwikkeling en onderhoud van de IT-omgeving. In andere gevallen kan een entiteit interne of

externe service providers gebruiken om bepaalde aspecten van, of IT-processen in, zijn IT-omgeving te beheren (bijvoorbeeld *hosting* door derden).

Het identificeren van IT-applicaties die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT

8. Door inzicht in de aard en complexiteit van de IT-omgeving van de entiteit, inclusief de aard en omvang van interne beheersingsmaatregelen voor informatieverwerking, kan de auditor bepalen op welke IT-applicaties de entiteit steunt om de integriteit van financiële informatie nauwkeurig te verwerken en te handhaven. De identificatie van IT-applicaties waarop de entiteit steunt, kan van invloed zijn op de beslissing van de auditor om de geautomatiseerde interne beheersingsmaatregelen binnen dergelijke IT-applicaties te toetsen, ervan uitgaande dat dergelijke geautomatiseerde interne beheersingsmaatregelen inspelen op geïdentificeerde risico's op een afwijking van materieel belang. Omgekeerd, als de entiteit niet steunt op een IT-applicatie, is het onwaarschijnlijk dat de geautomatiseerde interne beheersingsmaatregelen binnen een dergelijke IT-applicatie geschikt of voldoende nauwkeurig zijn ten behoeve van het toetsen van de effectieve werking. Geautomatiseerde interne beheersingsmaatregelen die kunnen worden geïdentificeerd in overeenstemming met paragraaf 26(b) kunnen bijvoorbeeld geautomatiseerde berekeningen of interne beheersingsmaatregelen over invoer, verwerking en uitvoer omvatten, zoals een aansluiting in drie richtingen van een inkooporder, verzending van een vervoersdocument en een leveranciersfactuur. Wanneer geautomatiseerde interne beheersingsmaatregelen door de auditor worden geïdentificeerd en de auditor bepaalt door het inzicht in de IT-omgeving dat de entiteit steunt op de IT-applicatie die deze geautomatiseerde interne beheersingsmaatregelen omvat, is het waarschijnlijker dat de auditor de IT-applicatie identificeert als een die onderhevig is aan risico's die voortkomen uit het gebruik van IT.

9. Bij het overwegen of de IT-applicaties waarvoor de auditor geautomatiseerde interne beheersingsmaatregelen heeft geïdentificeerd, onderhevig zijn aan risico's die voortkomen uit het gebruik van IT, zal de auditor waarschijnlijk overwegen of en de mate waarin de entiteit mogelijk toegang heeft tot de broncode waarmee het management programma wijzigingen kan maken in dergelijke interne beheersingsmaatregelen of de IT-applicaties. De mate waarin de entiteit programma- of configuratiewijzigingen maakt en de mate waarin de IT-processen over dergelijke wijzigingen zijn geformaliseerd, kunnen ook relevante overwegingen zijn. De auditor zal waarschijnlijk ook het risico op ongepaste toegang tot of wijzigingen in gegevens overwegen.

10. Door het systeem gegenereerde rapporten die de auditor voornemens is te gebruiken als controle-informatie, kunnen bijvoorbeeld een rapport over de ouderdom van handelsvorderingen of een rapport over de waardering van voorraden omvatten. Voor dergelijke rapporten kan de auditor controle-informatie verkrijgen over de volledigheid en nauwkeurigheid van de rapporten door gegevensgerichte werkzaamheden op de *inputs* en *outputs* van het rapport. In andere gevallen kan de auditor van plan zijn de effectieve werking van de interne beheersingsmaatregelen over het opstellen en het onderhoud van het rapport te toetsen, in welk geval de IT-applicatie waaruit het is geproduceerd, waarschijnlijk onderhevig is aan risico's die voortkomen uit het gebruik van IT. Naast het toetsen van de volledigheid en nauwkeurigheid van het rapport, kan de auditor van plan zijn om de effectieve werking van *general IT controls* die inspelen op risico's die verband houden met ongepaste of ongeautoriseerde programmawijzigingen of gegevenswijzigingen in het rapport, te toetsen.

11. Sommige IT-applicaties kunnen een functie voor het schrijven van rapporten bevatten, terwijl sommige entiteiten ook afzonderlijke applicaties voor het schrijven van rapporten (d.w.z. rapportgenerators) kunnen gebruiken. In dergelijke gevallen kan het nodig zijn dat de auditor de bronnen van door het systeem gegenereerde rapporten bepaalt (d.w.z. de applicatie die het

rapport opstelt en de gegevensbronnen die door het rapport worden gebruikt) om de IT-applicaties te bepalen die aan risico's onderhevig zijn die voortkomen uit het gebruik van IT.

12. De gegevensbronnen die door IT-applicaties worden gebruikt, kunnen databases zijn die bijvoorbeeld alleen toegankelijk zijn via de IT-applicatie of door IT-personeel met database beheerrechten. In andere gevallen kan de gegevensbron een datawarehouse zijn dat zelf kan worden beschouwd als een IT-applicatie onderhevig aan risico's die voortkomen uit het gebruik van IT.

13. De auditor kan een risico geïdentificeerd hebben waarvoor gegevensgerichte werkzaamheden alleen niet voldoende zijn vanwege het gebruik van in hoge mate geautomatiseerde en papierloze verwerking van transacties door de entiteit, wat betrekking kan hebben op meerdere geïntegreerde IT-applicaties. In dergelijke omstandigheden omvatten de door de auditor geïdentificeerde interne beheersingsmaatregelen waarschijnlijk geautomatiseerde interne beheersingsmaatregelen. Verder kan de entiteit steunen op *general IT-controls* om de integriteit van de verwerkte transacties en andere informatie die gebruikt is in de verwerking, te handhaven. In dergelijke gevallen zijn de IT-applicaties die betrokken zijn bij de verwerking en de opslag van de informatie waarschijnlijk onderhevig aan risico's die voortkomen uit het gebruik van IT.

Computergebruik door eindgebruikers

14. Hoewel controle-informatie ook kan komen in de vorm van door het systeem gegenereerde output die wordt gebruikt in een berekening uitgevoerd in een computerhulpmiddel voor eindgebruikers (bijv. spreadsheetsoftware of eenvoudige databases), worden dergelijke hulpmiddelen doorgaans niet geïdentificeerd als IT-applicaties in de context van paragraaf 26(b). Het opzetten en implementeren van interne beheersingsmaatregelen rond toegang en wijziging van computerhulpmiddelen voor eindgebruikers kan uitdagend zijn en dergelijke interne beheersingsmaatregelen zijn zelden gelijk aan of even effectief als *general IT controls*. In plaats daarvan kan de auditor een combinatie van beheersingsmaatregelen voor informatieverwerking overwegen, rekening houdend met het doel en de complexiteit van het betreffende computergebruik door eindgebruikers, zoals:

    - Interne beheersingsmaatregelen over informatieverwerking inzake de initiatie en verwerking van de brongegevens, inclusief relevante geautomatiseerde interne beheersingsmaatregelen of via interfaces tot het punt van waaruit de gegevens worden geëxtraheerd (dat wil zeggen het datawarehouse);
    - Interne beheersingsmaatregelen om te controleren of de logica werkt zoals bedoeld, bijvoorbeeld interne beheersingsmaatregelen die het extraheren van gegevens 'bewijzen', zoals het aansluiten van het rapport op de gegevens waarvan het is afgeleid, het vergelijken van de individuele gegevens uit het rapport met de bron en vice versa, en interne beheersingsmaatregelen die de formules of macro's controleren; of
    - Gebruik van validatie softwarehulpmiddelen, die formules of macro's controleren, zoals spreadsheet integriteitshulpmiddelen.

Schaalbaarheid

15. De mogelijkheid van de entiteit om de integriteit te handhaven van de informatie die in het informatiesysteem is opgeslagen en verwerkt, kan variëren op basis van de complexiteit en het aantal gerelateerde transacties en andere informatie. Hoe groter de complexiteit en het aantal gegevens dat een significante transactiestroom, rekeningsaldo of toelichting ondersteunt, hoe minder waarschijnlijk het wordt dat de entiteit de integriteit van die informatie handhaaft via interne

beheersingsmaatregelen voor informatieverwerking alleen (bijvoorbeeld interne beheersingsmaatregelen voor invoer en uitvoer of interne beheersingsmaatregelen voor beoordeling). Het wordt ook minder waarschijnlijk dat de auditor controle-informatie zal kunnen verkrijgen over de volledigheid en nauwkeurigheid van dergelijke informatie door gegevensgerichte werkzaamheden alleen wanneer dergelijke informatie wordt gebruikt als controle-informatie. In sommige omstandigheden, wanneer aantal en de complexiteit van transacties lager is, kan het management een interne beheersingsmaatregel over informatieverwerking hebben die voldoende is om de nauwkeurigheid en volledigheid van de gegevens te verifiëren (bijv. individuele verwerkte en gefactureerde verkooporders kunnen worden aangesloten met de *hard copy* die oorspronkelijk in de IT-applicatie is ingevoerd). Wanneer de entiteit steunt op general IT-controls om de integriteit van bepaalde informatie die door IT-applicaties wordt gebruikt, te handhaven, kan de auditor bepalen dat de IT-applicaties die die informatie onderhouden, onderhevig zijn aan risico's die voortkomen uit het gebruik van IT.

Voorbeeldkenmerken van een IT-applicatie die waarschijnlijk niet onderhevig is aan risico's die voortkomen uit IT	**Voorbeeldkenmerken van een IT-applicatie die waarschijnlijk onderhevig is aan risico's die voortkomen uit IT**
• Zelfstandige applicaties. • De hoeveelheid gegevens (transacties) is niet significant. • De functionaliteit van de applicatie is niet complex. • Elke transactie wordt ondersteund door originele *hard copy* documentatie.	• Applicaties zijn gekoppeld. • De hoeveelheid gegevens (transacties) is significant. • De functionaliteit van de applicatie is complex zoals: o De toepassing initieert automatisch transacties; en o Er zijn verschillende complexe berekeningen met onderliggende geautomatiseerde invoer.
De IT-applicatie is waarschijnlijk niet onderhevig aan risico's op IT omdat: • De hoeveelheid gegevens is niet significant en daarom steunt het management niet op *general IT controls* om de gegevens te verwerken of te onderhouden. • Het management steunt niet op geautomatiseerde interne beheersingsmaatregelen of andere geautomatiseerde functionaliteit. De auditor heeft geen geautomatiseerde interne beheersingsmaatregelen geïdentificeerd in overeenstemming met paragraaf 26(a). • Hoewel het management systeem-gegenereerde rapporten gebruikt in hun interne beheersingsmaatregelen, steunt het niet op deze rapporten. In plaats daarvan, sluit het de rapporten aan met de *hard copy* documentatie en verifieert het de berekeningen in de rapporten.	De IT-applicatie is waarschijnlijk onderhevig aan risico's op IT omdat: • Het management steunt op een applicatie systeem om gegevens te verwerken of te onderhouden als de hoeveelheid gegevens significant is. • Het management steunt op het applicatie systeem om bepaalde geautomatiseerde interne beheersingsmaatregelen uit te voeren die de auditor ook heeft geïdentificeerd.

• De auditor zal direct informatie toetsen die wordt geproduceerd door de entiteit die als controle-informatie wordt gebruikt.	

Andere aspecten van de IT-omgeving die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT

16. Wanneer de auditor IT-applicaties identificeert die onderhevig zijn aan risico's die voortkomen uit het gebruik van IT, zijn andere aspecten van de IT-omgeving doorgaans ook onderhevig aan risico's die voortkomen uit het gebruik van IT. De IT infrastructuur omvat de databases, het besturingssysteem en het netwerk. Databases slaan de gegevens die gebruikt worden door IT-applicaties op en kunnen bestaan uit vele onderling verbonden gegevenstabellen. Gegevens in databases kunnen ook rechtstreeks toegankelijk zijn via database managementsystemen door IT of ander personeel met database beheerrechten. Het besturingssysteem is verantwoordelijk voor het beheer van de communicatie tussen hardware, IT-applicaties en andere software die in het netwerk wordt gebruikt. Als zodanig kunnen IT-applicaties en databases direct toegankelijk zijn via het besturingssysteem. Een netwerk wordt gebruikt in de IT infrastructuur om gegevens te verzenden en informatie, middelen en diensten te delen via een gemeenschappelijke communicatielink. Het netwerk brengt doorgaans ook een logische beveiligingslaag tot stand (ingeschakeld via het besturingssysteem) voor toegang tot de onderliggende middelen.

17. Wanneer IT-applicaties door de auditor worden geïdentificeerd als onderhevig aan risico's die voortkomen uit IT, word(t)(en) de database(s) die de gegevens opslaat(n) die worden verwerkt door een geïdentificeerde IT-applicatie, meestal ook geïdentificeerd. Omdat de mogelijkheid voor de werking van een IT-applicatie vaak afhankelijk is van het besturingssysteem en de IT applicaties en databases direct toegankelijk kunnen zijn vanuit het besturingssysteem, is het besturingssysteem op gelijke manier meestal onderhevig aan risico's die voortkomen uit het gebruik van IT. Het netwerk kan worden geïdentificeerd wanneer het een centraal toegangspunt is voor de geïdentificeerde IT-applicaties en gerelateerde databases of wanneer een IT applicatie interactie heeft met leveranciers of externe partijen via het internet, of wanneer web-gerichte IT applicaties worden geïdentificeerd door de auditor.

Identificeren van risico's die voortkomen uit het gebruik van IT en general IT-controls

18. Voorbeelden van risico's die voortkomen uit het gebruik van IT omvatten risico's die verband houden met een ongepast steunen op IT applicaties die onnauwkeurig gegevens verwerken, onnauwkeurige gegevens verwerken, of beide, zoals:

    - Onbevoegde toegang tot gegevens die kan leiden tot vernietiging van gegevens of ongepaste wijzigingen in gegevens, inclusief het opnemen van ongeautoriseerde of niet-bestaande transacties of het onjuist vastleggen van transacties. Bijzondere risico's kunnen ontstaan wanneer meerdere gebruikers toegang hebben tot een gemeenschappelijke database.
    - De mogelijkheid voor IT-personeel om toegangsrechten te verkrijgen die verder gaan dan nodig is om hun toegewezen taken uit te voeren waardoor functiescheiding wordt doorbroken.
    - Onbevoegde wijzigingen in gegevens in hoofdbestanden.
    - Onbevoegde wijzigingen in IT-applicaties of andere aspecten van de IT-omgeving.
    - Het niet aanbrengen van noodzakelijke wijzigingen in IT-applicaties of andere aspecten van de IT-omgeving.
    - Ongepaste handmatige interventie.

- Potentieel verlies van gegevens of onmogelijkheid om toegang te krijgen tot gegevens zoals vereist.

19. De overweging van de auditor van onbevoegde toegang kan risico's met betrekking tot onbevoegde toegang omvatten door interne of externe partijen (vaak aangeduid als *cybersecurity*-risico's). Dergelijke risico's hoeven niet noodzakelijkerwijs invloed te hebben op de financiële verslaggeving, aangezien de IT-omgeving van een entiteit ook IT-applicaties en aanverwante gegevens kan omvatten die betrekking hebben op operationele of nalevingsbehoeften. Het is belangrijk op te merken dat cyberincidenten meestal eerst voorkomen via de omtrek en interne netwerklagen, die de neiging hebben verder verwijderd te zijn van de IT-applicatie, database en besturingssystemen die van invloed zijn op het opstellen van de financiële overzichten. Dienovereenkomstig, als informatie over een inbreuk op de beveiliging is geïdentificeerd, overweegt de auditor gewoonlijk in hoeverre een dergelijke inbreuk op de beveiliging de financiële verslaggeving zou kunnen beïnvloeden. Als de financiële verslaggeving hierdoor kan worden beïnvloed, kan de auditor besluiten inzicht te verwerven in de interne beheersingsmaatregelen en deze te toetsen om de mogelijke impact of reikwijdte van mogelijke afwijkingen in de financiële overzichten te bepalen of kan hij bepalen dat de entiteit voldoende toelichting heeft verstrekt over een dergelijke inbreuk op de beveiliging.

20. Wet- en regelgeving die een direct of indirect effect op de financiële overzichten van de entiteit heeft, kan bovendien gegevensbeschermingswetgeving omvatten. Overweging van de naleving van dergelijke wet- of regelgeving door een entiteit, in overeenstemming met ISA 250 (herzien) , kan inzicht in de IT processen van de entiteit en *general IT controls* die de entiteit heeft geïmplementeerd om de relevante wet- of regelgeving te adresseren, omvatten.

21. *General IT-controls* worden geïmplementeerd om in te spelen op risico's die voortkomen uit het gebruik van IT. Dienovereenkomstig gebruikt de auditor het verkregen inzicht in de geïdentificeerde IT-applicaties en andere aspecten van de IT-omgeving en de van toepassing zijnde risico's die voortkomen uit het gebruik van IT bij het bepalen van de te identificeren *general IT controls*. In sommige gevallen kan een entiteit gemeenschappelijke IT-processen over haar IT-omgeving gebruiken of tussen bepaalde IT-applicaties, in welk geval gemeenschappelijke risico's die voortkomen uit het gebruik van IT en algemene *general IT controls* kunnen worden geïdentificeerd.

22. In het algemeen kunnen waarschijnlijk een groter aantal *general IT controls* met betrekking tot IT-applicaties en databases worden geïdentificeerd dan voor andere aspecten van de IT-omgeving. Dit komt omdat deze aspecten het meest betrokken bij de informatieverwerking en opslag van informatie in het informatiesysteem van de entiteit. Bij het identificeren van *general IT controls* kan de auditor de interne beheersing van handelingen van zowel eindgebruikers als van het IT-personeel van de entiteit of IT-serviceproviders overwegen.

23. **Bijlage 6** geeft een nadere toelichting op de aard van de *general IT controls* doorgaans geïmplementeerd voor verschillende aspecten van de IT-omgeving. Bovendien worden voorbeelden van *general IT controls* voor verschillende IT-processen gegeven.

Bijlage 6

(Zie par. 26(c), A173-A174)

Overwegingen voor het verwerven van inzicht in *general IT controls*

Deze bijlage bevat verdere aangelegenheden die de auditor kan overwegen bij het verwerven van inzicht in *general IT controls*

1. De aard van de *general IT controls* die doorgaans worden geïmplementeerd voor elk aspect van de IT omgeving:

   (a) Applicaties

   General IT-controls op de IT-applicatielaag hangen samen met de aard en omvang van applicatiefunctionaliteit en de toegangspaden die zijn toegestaan in de technologie. Bijvoorbeeld meer interne beheersingsmaatregelen zullen relevant zijn voor in hoge mate geïntegreerde IT-applicaties met complexe beveiligingsopties dan een verouderde IT-applicatie die een klein aantal rekeningsaldi ondersteunt met toegangsmethoden alleen via transacties.

   (b) Database

   General IT-controls op de databaselaag spelen typisch op de risico's in die voortkomen uit het gebruik van IT gerelateerd aan ongeautoriseerde updates van financiële verslaggevingsinformatie in de database via direct database toegang of uitvoering van een script of programma.

   (c) Besturingssysteem

   General IT-controls op de laag van het besturingssysteem spelen doorgaans in op risico's die voortkomen uit het gebruik van IT met betrekking tot beheerderstoegang, wat het doorbreken van andere interne beheersingsmaatregelen kan faciliteren. Dit omvat handelingen zoals het in gevaar brengen van de inloggegevens van andere gebruikers, het toevoegen van nieuwe, ongeautoriseerde gebruikers, laden van malware of uitvoeren van scripts of andere ongeautoriseerde programma's.

   (d) Netwerk

   General IT-controls op de netwerklaag spelen doorgaans in op risico's die voortkomen uit het gebruik van IT gerelateerd aan netwerksegmentatie, toegang op afstand en authenticatie. Netwerk beheersmaatregelen kunnen relevant zijn wanneer een entiteit web-gerichte applicaties heeft die worden gebruikt voor financiële verslaggeving. Netwerk beheersmaatregelen kunnen ook relevant zijn wanneer de entiteit significante relaties met zakenpartners heeft of uitbesteding door derden, waardoor gegevensoverdrachten en de noodzaak van toegang op afstand kunnen toenemen.

2. Voorbeelden van general IT-controls die kunnen bestaan, georganiseerd door IT-processen, omvatten:

   (a) Proces om toegang te beheren:

- *Authenticatie*

  Interne beheersingsmaatregelen die ervoor zorgen dat een gebruiker die toegang heeft tot de IT-applicatie of een ander aspect van de IT omgeving, de eigen inloggegevens van de gebruiker gebruikt (dat wil zeggen, de gebruiker gebruikt inloggegevens van andere gebruikers).

- *Autorisatie*

  Interne beheersingsmaatregelen die gebruikers toestaat om toegang hebben tot de informatie die nodig is voor hun taakverantwoordelijkheden en verder niets, wat een passende functiescheiding mogelijk maakt.

- *Toegang verlenen*

  Interne beheersingsmaatregelen om nieuwe gebruikers te autoriseren en wijzigingen in de toegangsrechten van bestaande gebruikers.

- *Toegang opheffen*

  Interne beheersingsmaatregelen om gebruikerstoegang te verwijderen bij beëindiging of overdracht.

- *Toegangsprivileges*

  Interne beheersingsmaatregelen over de toegang van beheerders of krachtige gebruikers.

- *Beoordelingen van gebruikerstoegang*

  Interne beheersingsmaatregelen om gebruikerstoegang opnieuw te certificeren of te evalueren voor doorlopende autorisatie in de loop van de tijd.

- *Interne beheersingsmaatregelen over beveiligingsconfiguratie*

  Elke technologie heeft over het algemeen belangrijke configuratie-instellingen die helpen de toegang tot de omgeving te beperken.

- *Fysieke toegang*

  Interne beheersingsmaatregelen over fysieke toegang tot het datacenter en hardware, omdat dergelijke toegang gebruikt kan om andere interne beheersingsmaatregelen te doorbreken.

(b) Proces om programma- of andere wijzigingen in de IT-omgeving te beheren:

- *Change management proces*

  Interne beheersingsmaatregelen over het proces om wijzigingen naar een productie (d.w.z. eindgebruiker) omgeving op te zetten, te programmeren, te toetsen en te migreren.

- *Functiescheiding over wijzigingsmigratie*

  Interne beheersingsmaatregelen die toegang scheiden om wijzigingen in een productieomgeving aan te brengen.

- *Systeemontwikkeling of acquisitie of implementatie*

  Interne beheersingsmaatregelen over de initiële ontwikkeling of implementatie van IT-applicaties (of in relatie tot andere aspecten van de IT-omgeving).

- *Data conversie*

  Interne beheersingsmaatregelen over de conversie van gegevens tijdens ontwikkeling, implementatie of upgrades naar de IT-omgeving.

(c) Proces om IT-activiteiten te beheren

- *Taakplanning*

  Interne beheersingsmaatregelen over de toegang om taken of programma's te plannen en te initiëren die gevolgen kunnen hebben voor de financiële verslaggeving.

- *Taakmonitoring*

  Interne beheersingsmaatregelen om financiële verslaggevingstaken of -programma's te monitoren voor succesvolle uitvoering.

- *Back-up en herstel*

  Interne beheersingsmaatregelen om ervoor te zorgen dat back-ups van financiële verslaggevingsgegevens plaatsvinden zoals gepland en zodat gegevens beschikbaar zijn en kunnen worden geraadpleegd voor tijdig herstel in geval van een storing of aanval.

- *Indringersdetectie*

  Interne beheersingsmaatregelen om te monitoren op kwetsbaarheden en/of inbraken in de IT-omgeving.

De onderstaande tabel illustreert voorbeelden van *general IT controls* om in te spelen op voorbeelden van risico's die voortkomen uit het gebruik van IT, inclusief verschillende IT-applicaties op basis van hun aard.

Proces	**Risico's**	**Interne beheersings-maatregelen**	**IT-applicaties**		
IT proces	**Voorbeeld-risico's die voortkomen uit het gebruik van IT**	**Voorbeeld general IT-controls**	**Niet-complexe commerciële software - Van toepassing (Ja nee)**	**Middelgrote en matig complex commerciële software of IT applicaties - Van toepassing (Ja/ nee)**	**Grote of complexe IT applicaties (bijvoorbeeld ERP systemen) - Van toepassing (Ja/ nee)**
Toegang beheren	Gebruikers-toegangs-privileges:	Management keurt de aard en omvang	Ja - in plaats van beoordelingen	Ja	Ja

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

	Gebruikers hebben toegangs-privileges die verder gaan dan degenen die nodig zijn om hun toegewezen taken uit te voeren, hetgeen ongepaste functiescheidi ng kan creëren.	van gebruikers toegangs-privileges voor nieuwe en aangepast gebruikers-toegang goed, inclusief standaard applicatie profielen / rollen, kritisch financiële verslaggeving s-transacties, en functiescheidi ng	van gebruikers-toegang hieronder		
		Toegang voor beëindigde of overgedragen gebruikers is tijdig verwijderd of gewijzigd	Ja - in plaats van beoordelingen van gebruikers-toegang hieronder	Ja	Ja
		Gebruikers-toegang wordt periodiek beoordeeld	Ja - in plaats van interne beheersingsm aat-regelen over toegang verlenen/ophe ffenhierboven	Ja voor bepaalde applicaties	Ja
		Functiescheidi ng wordt gemonitord en conflicterende toegang wordt verwijderd of toegewezen aan mitigerende interne beheersingsm aat-regelen, die zijn gedocumente erd en getoetst	Nvt - geen systeem ingeschakelde scheiding	Ja voor bepaalde applicaties	Ja

		Toegang oo Privilege-niveau (bijv. configuratie, gegevens en veiligheids-beheerders) is geautoriseerd en op gepaste wijze beperkt	Ja - waarschijnlijk alleen bij IT-applicatie-laag	Ja - bij IT applicatie en bepaalde lagen van IT omgeving voor een platform	Ja op alle lagen van IT omgeving voor een platform
Toegang beheren	Directe gegevens toegang: Ongepaste veranderingen zijn rechtstreeks gemaakt aan financiële data door andere middelen dan applicatie transacties.	Toegang tot applicatie gegevens-bestanden of database objecten / tabellen / gegevens is beperkt tot geautoriseerd personeel op basis van hun taakverantwo ordelijkheden en toegewezen rol, en dergelijke toegang is goedgekeurd door het management	Nvt	Ja voor bepaalde applicaties en databases	Ja
Toegang beheren	Systeem instellingen: Systemen zijn niet voldoende geconfigureer d of bijgewerkt om systeemtoega ng te beperken tot naar behoren geautoriseerd e en geschikte gebruikers.	Toegang is geverifieerddo or unieke gebruikersID's en wachtwoorden of andere methoden zoals een mechanisme voor het valideren dat gebruikers geautoriseerd zijn om toegang krijgen tot het systeem. Wachtwoord	Ja - alleen wachtwoord authenticatie	Ja - mix van wachtwoord en multi-factor authenticatie	Ja

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

		parameters voldoen aan de bedrijfs- of sector normen (bijv. minimum lengte wachtwoord en complexiteit, vervaldatum, account-vergrendeling)			
		De belangrijkste kenmerken van de bewakings-configuratie zijn op gepaste wijze geïmplementeerd	Nvt - er bestaan geen technische veiligheids-configuraties	Ja voor bepaalde applicaties en databases	Ja
Wijzigingen beheren	Applicatie wijzigingen: Ongepaste wijzigingen zijn gemaakt aan applicatie-systemen of programma's die relevante geautomatiseerd interne beheersingsmaat-regelen bevatten (d.w.z. configureerbare instellingen, geautomatiseerde algoritmen, geautomatiseerde berekeningen en geautomatiseerde data-extractie) of rapport logica.	Applicatie wijzigingen zijn passend getoetst en goedgekeurd voordat ze verplaatst worden naar de productie omgeving	Nvt - zou verifiëren dat er geen broncode is geïnstalleerd	Ja - voor niet-commerciële software	Ja
		Toegang tot wijzigingen doorvoeren in de applicatie productie omgeving is op gepaste wijze beperkt en gescheiden van de ontwikkel omgeving	Nvt	Ja voor niet-commerciële software	Ja

Wijziging beheren	Database wijzigingen: Ongepaste wijzigingen zijn gemaakt in de database structuur en relaties tussen de gegevens.	Database wijzigingen zijn passend getoetst en goedgekeurd voordat ze verplaatst worden naar de productie omgeving	Nvt - nee database veranderingen gemaakt bij de entiteit	Ja - voor niet-commerciële software	Ja
Wijzigingen beheren	Systeem software wijzigingen: Ongepaste wijzigingen zijn gemaakt in systeem software (bijv. besturings-systeem, netwerk, *change management* software, toegangscontrole software).	Systeem software wijzigingen zijn op passende wijze getoetst en goedgekeurd voordat ze worden verplaatst naar de productie	Nvt - geen systeem software wijzigingen zijn gemaakt bij entiteit	Ja	Ja
Wijzigingen beheren	Gegevens conversie: Gegevens geconverteerd uit verouderde systemen of voorgaande versies introduceren fouten in gegevens als de conversie incomplete, overtollige, verouderde, of onnauwkeurige gegevens overbrengt.	Management keurt de resultaten goed van de conversie van gegevens (bijvoorbeeld balans-opmakende en aansluitings-activiteiten) van het oude applicatie systeem of de gegevens structuur naar het nieuwe applicatiesysteem of de gegevens-structuur en monitort dat de conversie is uitgevoerd	Nvt - behandeld door handmatige interne beheersingsmaat-regelen	Ja	Ja

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

		in overeenstemming met vastgestelde conversie-beleidslijnen en procedures			
IT activiteiten	Netwerk: het netwerk voorkomt onvoldoende dat onbevoegde gebruikers ongepast toegang verkrijgen tot informatie systemen.	Toegang is geauthentiseerd door unieke gebruikers-ID's en wachtwoorden of andere methoden zoals een mechanisme voor het valideren dat gebruikers geautoriseerd zijn om toegang te krijgen tot het systeem. Wachtwoord parameters voldoen aan bedrijfs- of professionele beleidslijnen en normen (bijv. minimum lengte wachtwoord en complexiteit, vervaldatum, account-vergrendeling)	Nvt - er bestaat geen aparte netwerk authenticatie methode	Ja	Ja
		Netwerk is ontworpen voor gesegmenteerde web-gerichte applicaties van het interne netwerk, waar ICFR	Nvt - geen netwerk segmentatie toegepast	Ja - met oordeelsvorming	Ja - met oordeelsvorming

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

		relevante applicaties toegankelijk zijn			
		Kwetsbaarheids-scans van de netwerk omtrek worden periodiek uitgevoerd door het netwerk management team, dat ook potentiële kwetsbaarheden onderzoekt	Nvt	Ja - met oordeelsvorming	Ja - met oordeelsvorming
		Waarschuwingen worden periodiek gegenereerd om kennisgeving van bedreigingen die zijn geïdentificeerd door de inbreuk detectiesystemen te verschaffen. Deze bedreigingen zijn onderzocht door het netwerk management team	Nvt	Ja - met oordeelsvorming	Ja - met oordeelsvorming
		Interne beheersingsmaatregelen zijn geïmplementeerd om *Virtual Private Network* (VPN) toegang tot geautoriseerd	Nvt - geen VPN	Ja - met oordeelsvorming	Ja - met oordeelsvorming

Originele bron: *Handbook of International Quality Management, Auditing, Review, Other Assurance, and Related Services Pronouncements, 2023-2024 Edition Volume I*

		e en geschikte gebruikers te beperken			
IT Activiteiten	Gegevens back-up en herstel: Financiële gegevens kunnen niet tijdig worden hersteld of benaderd bij een verlies van gegevens.	Er wordt regelmatig een back-up gemaakt van financiële gegevens volgens een vastgesteld schema en frequentie	Nvt - steunend op handmatige back-ups door het financiële team	Ja	Ja
IT Activiteiten	Taakplanning: Productie systemen, programma's, of taken resulteren in onnauwkeurig, onvolledig, of ongeautoriseerd verwerken van gegevens.	Alleen geautoriseerde gebruikers hebben toegang om de batch taken bij te werken (inclusief interface-taken) in de taakplannings - software	Nvt - geen batch taken	Ja voor bepaalde applicaties	Ja
		Kritische systemen, programma's of taken worden gemonitord en verwerkings-fouten worden gecorrigeerd om te zorgen voor succesvolle implementatie.	Nvt - geen taakmonitoring	Ja voor bepaalde applicaties	Ja