NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

NOREA Richtijn 3402

ASSURANCE-RAPPORTEN BETREFFENDE INTERNE BEHEERSINGSMAATREGELEN BIJ EEN SERVICEORGANISATIE

(Van toepassing op assurance-rapporten van IT-auditors van de serviceorganisatie over verslagperioden eindigend op of na 15 juni 2011; aangepast voor opdrachten die aanvangen na 1 janari 2017, naar aanleiding van herziene Richtlijn 3000A)

Deze vaktechnische Richtlijn is een Nederlandse vertaling van International Standard on Auditing 3402 'Assurance reports on controls at a Service organization'. Deze vertaling is tot stand gekomen in nauwe samenwerking met NBA (Nederlandse Beroepsorganisatie van Accountants). De tekst van deze Richtlijn 3402 komt overeen met de tekst van Standaard 3402 van NBA met uitzondering van aanduiding van het document (Richtlijn versus Standaard), aanduiding beroepsbeoefenaar (IT-auditor versus accountant) en eventuele verwijzingen naar specifieke andere voorschriften van de desbetreffende beroepsgroep. NB: op enkele plaatsen wordt in deze Richtlijn verwezen naar specifieke standaarden voor opdrachten tot controle van historische financiële informatie die zijn uitgegeven door NBA.

Deze herziene richtlijn is vastgesteld in de algemene ledenvergadering van NOREA van 14 december 2016.

INHOUD

Inleiding

Toepassingsgebied van deze Richtlijn

1. Deze Richtlijn behandelt de assurance-opdrachten die door een beroepsbeoefenaar[1] worden uitgevoerd om voor gebruikersorganisaties en hun accountants een rapportage te verstrekken. Deze rapportage betreft de interne beheersingsmaatregelen van een serviceorganisatie die aan de gebruikersorganisaties een dienst verleent die waarschijnlijk relevant is voor de interne beheersing van de gebruikersorganisaties in relatie tot de financiële verslaggeving. Deze Richtlijn vult Standaard 402 van NBA en ISA 402 van IFAC aan zodat de rapportages opgesteld in overeenstemming met deze Richtlijn, geschikt zijn de onder Standaard/ISA 402[2] passende assurance-informatie te verschaffen. (Zie Par. A1.)

2. In het "Stramien voor Assurance-opdrachten" (het Stramien) staat aangegeven dat een assurance-opdracht een opdracht met een "redelijke mate van zekerheid" of een opdracht met een beperkte mate van zekerheid" kan zijn, dat een assurance-opdracht een attest-opdracht of een directe-opdracht kan zijn[3]. In deze Standaard worden alleen attest-opdrachten met een redelijke mate van zekerheid behandeld.

3. Deze Richtlijn is alleen van toepassing wanneer de serviceorganisatie verantwoordelijk is voor, of anderszins in staat is om een vermelding te doen over de geschikte opzet van interne beheersingsmaatregelen. In deze Richtlijn worden niet de assurance-opdrachten behandeld:

   (a) om uitsluitend te rapporteren over de vraag of interne beheersingsmaatregelen van een serviceorganisatie zo werken als staat beschreven; of
   (b) om te rapporteren over interne beheersingsmaatregelen van een serviceorganisatie anders dan die beheersmaatregelen die verband houden met een dienst die waarschijnlijk relevant is voor de interne beheersing van de gebruikersorganisaties in relatie tot de financiële verslaggeving (bijvoorbeeld, interne beheersingsmaatregelen die de productie of kwaliteitsbeheersing van de gebruikersorganisaties beïnvloeden).

   Desalniettemin worden in deze Richtlijn enige leidraden verschaft voor dergelijke opdrachten die onder Richtlijn 3000A worden uitgevoerd. (Zie Par. A2)

4. Naast het uitbrengen van het assurance-rapport betreffende interne beheersingsmaatregelen kan een IT-auditor van de serviceorganisatie ook ingehuurd zijn om rapporten te verschaffen, die niet in deze Richtlijn behandeld worden zoals de volgende:

   (a) Een rapportage betreffende de transacties of saldi van een gebruikersorganisatie die door een serviceorganisatie worden onderhouden; of
   (b) Een rapport van feitelijke bevindingen betreffende de interne beheersingsmaatregelen van een serviceorganisatie.

Relatie met Richtlijn 3000A, overige professionele uitingen en overige vereisten

5. De IT-auditor van de serviceorganisatie dient Richtlijn 3000A en deze Richtlijn na te leven bij de uitvoering van assurance-=opdrachten voor interne beheersingsmaatregelen bij een service-organisatie. Deze Richtlijn vult Richtlijn 3000A aan, maar is hier geen vervanging voor en zet uiteen op welke wijze Richtlijn 3000A toegepast moet worden op een assurance-opdracht met een redelijke mate van zekerheid om over de interne beheersingsmaatregelen van een serviceorganisatie te rapporteren.3000A3000A3000A

6. Het naleven van Richtlijn 3000A vereist onder andere IT-auditornaleving van het Reglement Gedragscode ('Code of Ethics') of – indien van toepassing- andere wettelijke of professionele vereisten, die ten minste gelijkwaardig zijn. [6]. Het is tevens vereist van de opdrachtpartner dat hij werkzaam is bij of verbonden is aan een IT-auditeenheid die onderworpen is aan het Reglement Kwaliteitsbeheersing NOREA (RKBN) of regelgeving die ten minste gelijkwaardig is. [7]

Ingangsdatum

7. Deze herziene Richtlijn is van toepassing op assurance-rapporten van IT-auditors van de serviceorganisatie voor opdrachten die aanvangen na 1 januari 2017, naar aanleiding van herziene Richtlijn 3000A.

Doelstellingen

8. De doelstellingen van de IT-auditor van de serviceorganisatie zijn:

(a) Het verkrijgen van een redelijke mate van zekerheid over de vraag of, in alle van materieel belang zijnde opzichten, op basis van geschikte criteria:

(i) De beschrijving van de serviceorganisatie van haar systeem, het systeem getrouw weergeeft zoals dit gedurende de gespecificeerde verslagperiode is opgezet en geïmplementeerd (of in het geval van een type 1 rapport, op een gespecificeerde datum);

(ii) De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die staan vermeld in de beschrijving van de serviceorganisatie van haar systeem gedurende de gespecificeerde verslagperiode op afdoende wijze zijn opgezet (of in het geval van een type 1 rapport, op een gespecificeerde datum);

(iii) Waar inbegrepen in de reikwijdte van de opdracht, de interne beheersingsmaatregelen, , effectief werkten om een redelijke mate van zekerheid te verschaffen dat de interne beheersingsdoelstellingen die in de beschrijving van het systeem van de serviceorganisatie staan vermeld, gedurende de gespecificeerde verslagperiode zijn bereikt.

(b) Te rapporteren over de aangelegenheden die hierboven bij (a) staan vermeld in overeenstemming met de bevindingen van de IT-auditor van de serviceorganisatie.

[1] Richtlijn 3000A (herzien) asurance-opdrachten door IT-auditors (attest-opdrachten), paragraaf 12(r)IT-auditor
[2] NBA Standaard 402, "Overwegingen met betrekking tot controles van entiteiten die gebruikmaken van een serviceorganisatie".
[3] Richtlijn 3000A paragraaf 12.
[4] Paragraaf 13 en 52 (k) van deze Richtlijn.
3000AIT-auditor[6] Richtlijn 3000A, paragrafen 3(a), 20 en 34
[7] Richtlijn 3000A, paragraaf 3(b), en 31a

Definities

9. In het kader van deze Standaard hebben de volgende termen de hierna weergegeven betekenissen:

(a) Uitsluitingsmethode (Carve-out methode) – een methode van omgaan met de diensten die worden verleend door een subserviceorganisatie. Hierbij omvat de beschrijving van de serviceorganisatie van haar systeem de aard van de diensten die door een subserviceorganissatie worden verleend. De relevante interne beheersingsdoelstellingen en de daarmee verband houdende interne beheersingsmaatregelen van de subserviceorganisatie zijn echter uitgesloten van de beschrijving van de serviceorganisatie van haar systeem alsmede van de reikwijdte van de opdracht van de IT-auditor van de serviceorganisatie. De beschrijving van de serviceorganisatie van haar systeem en de reikwijdte van de opdracht van de IT-auditor van de serviceorganisatie bevatten interne beheersingsmaatregelen van de serviceorganisatie die de effectiviteit van de interne beheersingsmaatregelen van een subserviceorganisatie monitort, wat in kan houden dat de serviceorganisatie een assurance- rapport betreffende de interne beheersingsmaatregelen van de subserviceorganisatie beoordeelt.

(b) Aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie – Interne beheersingsmaatregelen waarvan de serviceorganisatie, bij het opzetten van de dienst, aanneemt dat zij door de gebruikersorganisaties zullen worden geïmplementeerd en die, indien noodzakelijk om de interne beheersingsdoelstellingen te bereiken, in de beschrijving van de serviceorganisatie van haar systeem staan vermeld.

(c) Interne beheersingsdoelstelling – Het doel of doeleinde van een bepaald aspect van interne beheersingsmaatregelen. Interne beheersingsdoelstellingen houden verband met risico's waar de interne beheersingsmaatregelen naar streven deze te mitigeren.

(d) Interne beheersingsmaatregelen bij de serviceorganisatie – Interne beheersingsmaatregelen over het bereiken van een interne beheersingsdoelstelling die door het assurance-rapport van de IT-auditor wordt omvat. (Zie Par. A3)

(e) Interne beheersingsmaatregelen van een subserviceorganisatie – Interne beheersingsmaatregelen van een subserviceorganisatie die een redelijke mate van zekerheid verschaffen over het bereiken van een interne beheersingsdoelstelling.

(f) Criteria – Benchmarks die gebruikt worden om het object van onderzoek te evalueren of te meten. De 'van toepassing zijnde criteria' zijn de criteria die bij de specifieke opdracht worden gebruikt..

(g) Opname methode (Inclusive methode) – Methode hoe er wordt omgegaan met de diensten die door een subserviceorganisatie worden verleend. Hierbij omvat de beschrijving van de serviceorganisatie van haar systeem de aard van de diensten die door de subserviceorganisatie worden verleend. De relevante interne beheersingsdoelstellingen van die subserviceorganisatie en daarmee verband houdende interne beheersingsmaatregelen zijn opgenomen in de beschrijving van de serviceorganisatie van haar systeem en in de reikwijdte van de opdracht van de IT-auditor van de serviceorganisatie. (Zie Par. A4)

(h) Interne auditfunctie – Een functie van een entiteit die assurance- en adviesactiviteiten uitvoert die zijn opgezet om de effectiviteit van de governance, risicobeheersings- en interne beheersingsprocessen van de entiteit te evalueren en te verbeteren..

(i) Interne IT-auditors – Die individuen die de activiteiten van de interne auditfunctie uitvoeren. Interne IT-auditors kunnen tot een interne auditafdeling of vergelijkbare functie behoren.

(j) Een rapportage over de beschrijving en de opzet van interne beheersingsmaatregelen van een serviceorganisatie (in deze Richtlijn wordt daarnaar verwezen als een "type 1 rapport") – Een rapportage die bestaat uit:

(i) De beschrijving van de serviceorganisatie van haar systeem;

(ii) Een schriftelijke vermelding van de serviceorganisatie dat, in alle van materieel belang zijnde opzichten, en op basis van geschikte criteria:

a. de beschrijving het systeem van de serviceorganisatie getrouw weergeeft zoals dit is opgezet en geïmplementeerd op de gespecificeerde datum;

b. de interne beheersingsmaatregelen die verband houden met interne beheersingsdoelstellingen zoals die in de beschrijving van de serviceorganisatie van haar systeem op de gespecificeerde datum staan vermeld, op afdoende wijze zijn opgezet; en

(iii) een assurance-rapport van de IT-auditor van de serviceorganisatie dat een conclusie met een redelijke mate van zekerheid over de aangelegenheden in (ii)a.-b. hierboven uitdrukt.

(k) Rapport over de beschrijving, opzet en werking van de interne beheersingsmaatregelen van een serviceorganisatie (in deze Richtlijn wordt daarnaar verwezen als een "type 2 rapport") – Een rapport dat bestaat uit:

(i) de beschrijving van de serviceorganisatie van haar systeem;

(ii) een schriftelijke vermelding van de serviceorganisatie dat in alle van materieel belang zijnde opzichten, en op basis van geschikte criteria:

a. de beschrijving het systeem van de serviceorganisatie getrouw weergeeft zoals deze gedurende de gespecificeerde verslagperiode is opgezet en geïmplementeerd;

b. de interne beheersingsmaatregelen die verband houden met interne beheersingsdoelstellingen zoals die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, gedurende de gespecificeerde verslagperiode op afdoende wijze zijn opgezet; en

c. de interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen zoals die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, gedurende de gespecificeerde verslagperiode effectief werkten; en

(iii) Een assurance-rapport van de IT-auditor van de serviceorganisatie dat:

a. een conclusie met een redelijke mate van zekerheid over de aangelegenheden in (ii)a.-c. hierboven uitdrukt; en

b. een beschrijving van de toetsingen van interne beheersingsmaatregelen en de resultaten daarvan omvat.

(l) IT-auditor van de serviceorganisatie – Een beroepsbeoefenaar die, op verzoek van de serviceorganisatie, een assurance-rapport verstrekt betreffende de interne beheersingsmaatregelen van een serviceorganisatie.

(m) Serviceorganisatie – Een derde organisatie (of onderdeel van een derde organisatie) die diensten verleent aan gebruikersorganisaties die waarschijnlijk relevant zijn voor de interne beheersing in relatie tot de financiële verslaggeving.

(n) Systeem van een serviceorganisatie (of het systeem) – De beleidslijnen en procedures die door de serviceorganisatie zijn opgezet en geïmplementeerd om de gebruikersorganisaties de diensten te verlenen die door het assurance-rapport van de IT-auditor van de serviceorganisatie worden omvat. De beschrijving van de serviceorganisatie van haar systeem bestaat onder meer uit het identificeren van: de diensten die worden verleend; de verslagperiode, of in het geval van een type 1 rapport de datum waarop de beschrijving betrekking heeft; interne beheersingsdoelstellingen; en daarmee verband houdende interne beheersingsmaatregelen.

(o) Vermelding van een serviceorganisatie – De schriftelijke vermelding over de aangelegenheden waarnaar in paragraaf 9(k)(ii) (of in het geval van een type 1 rapport in paragraaf 9 (j)(ii)) wordt verwezen.

(p) Subservice organisatie – Een serviceorganisatie die door een andere serviceorganisatie wordt gebruikt om sommige diensten uit te voeren die aan gebruikersorganisaties worden verleend die waarschijnlijk relevant zijn voor de interne beheersing van gebruikersorganisaties in relatie tot de financiële verslaggeving.

(q) Toetsing van interne beheersingsmaatregelen – Een controlemaatregel die is opgezet om de werking van interne beheersingsmaatregelen voor het bereiken van de interne beheersingsdoelstellingen, zoals vermeld in de beschrijving van het systeem van de serviceorganisatie, te evalueren.

(r) Accountant van de gebruiker – Een accountant die de financiële overzichten van een gebruikersorganisatie controleert en daarover verslag uitbrengt[7].

(s) Gebruikersorganisatie– Een entiteit die gebruik maakt van een serviceorganisatie.

Vereisten

Richtlijn 3000A

10. De IT-auditor van de serviceorganisatie dient niet aan te geven conform deze Richtlijn te hebben gewerkt, tenzij de IT-auditor van de serviceorganisatie de vereisten van deze Richtlijn en Richtlijn 3000A heeft nageleefd.

Ethische voorschriften

11. De IT-auditor van de serviceorganisatie dient het Reglement Gedragscode (‘Code of Ethics’) in relatie tot assurance-opdrachten na te leven, of –indien van toepassing- andere wettelijke of professionele vereisten, die ten minste gelijkwaardig zijn. (Zie Par. A5)

Management en degenen belast met governance

12. Waar op grond van deze Richtlijn van de IT-auditor van de serviceorganisatie vereist wordt dat hij verzoekt om inlichtingen van, of bevestigingen verzoekt bij, communiceert met, of anderszins in interactie staat met de serviceorganisatie, dient de IT-auditor van de serviceorganisatie de juiste persoon of personen binnen het management van de serviceorganisatie of governancestructuur met wie die interactie plaatsvindt te bepalen. Dit dient onder meer in te houden het beschouwen van welke persoon of personen de geschikte verantwoordelijkheden voor en kennis van de betrokken aangelegenheden hebben. (Zie Par. A6)

Aanvaarding en continuering

13. Alvorens de IT-auditor van de serviceorganisatie een opdracht aanvaardt of continueert, dient hij:

(a) Te bepalen of:

(i) De IT-auditor van de serviceorganisatie de capaciteiten en de competentie bezit om de opdracht uit te voeren; (Zie Par. A7)

(ii) De toe te passen criteria bij de serviceorganisatie waarvan de IT-auditor veronderstelt dat deze om de beschrijving van haar systeem op te stellen, voor de gebruikersorganisaties en hun accountants geschikt zijn en beschikbaar zullen zijn; en

(iii) De reikwijdte van de opdracht en de beschrijving van de serviceorganisatie van haar systeem niet zo beperkt zullen zijn dat het onwaarschijnlijk is dat zij voor de gebruikersorganisaties en hun accountants nuttig zijn.

(b) De instemming van de serviceorganisatie te verkrijgen dat zij haar verantwoordelijkheid erkent en begrijpt:

(i) Voor het opstellen van de beschrijving van haar systeem en de bijgaande vermelding van de serviceorganisatie, inclusief de volledigheid, nauwkeurigheid zijn en de methode van presentatie van die beschrijving en vermelding; (Zie Par. A8)

(ii) Om een redelijke basis te hebben voor de vermelding van de serviceorganisatie die met de beschrijving van haar systeem samengaat: (Zie Par. A9)

(iii) Voor het in de vermelding van de serviceorganisatie aangeven van de criteria die zij hanteerde bij het beschrijven van haar systeem;

(iv) Voor het in de beschrijving van haar systeem aangeven van:

a. De interne beheersingsdoelstellingen; en

b. De partij die deze doelstellingen specificeerde wanneer deze gespecificeerd zijn door wet- of regelgeving, of een andere partij (bijvoorbeeld een gebruikersgroep of een beroepsorganisatie);

(v) Voor het identificeren van risico's die het bereiken van interne beheersingsdoelstellingen die in de beschrijving van haar systeem staan vermeld in gevaar brengen, en het opzetten en implementeren van interne beheersingsmaatregelen om een redelijke mate van zekerheid te verschaffen dat die risico's het bereiken van de interne beheersingsdoelstellingen die in de beschrijving van haar systeem staan aangegeven niet zullen verhinderen, en daarmee dat de aangegeven interne beheersingsdoelstellingen zullen worden bereikt; en (Zie Par. A10)

(vi) Om de IT-auditor van de serviceorganisatie:

a. Toegang te verschaffen tot alle informatie zoals vastleggingen, documentatie en andere aangelegenheden, met inbegrip van service level agreements waarvan de serviceorganisatie op de hoogte is dat deze relevant is voor de beschrijving van het systeem van de serviceorganisatie en de bijgaande vermelding van de serviceorganisatie;

b. Aanvullende informatie te verschaffen die de IT-auditor kan verzoeken aan de serviceorganisatie voor de doeleinden van de assurance-opdracht; en

c. Onbeperkte toegang te verschaffen tot de personen binnen de serviceorganisatie van wie IT-auditor van de serviceorganisatie bepaalt dat het noodzakelijk is assurance-informatie te verkrijgen.

De aanvaarding van een wijziging in de voorwaarden van de opdracht.

14. Indien de serviceorganisatie voor de afronding van de opdracht verzoekt om een wijziging in de reikwijdte van de opdracht, dient de IT-auditor van de serviceorganisatie zich ervan te vergewissen dat er een redelijke rechtvaardiging bestaat voor die wijziging. (Zie Par. A11 en A12)

De geschiktheid van de criteria bepalen

15. 3000ADe IT-auditor van de serviceorganisatie dient te bepalen of de serviceorganisatie geschikte criteria heeft gehanteerd bij het opstellen van de beschrijving van haar systeem, bij het evalueren of de interne beheersingsmaatregelen op afdoende wijze zijn opgezet en, in het geval van een type 2 rapport, bij het evalueren of de interne beheersingsmaatregelen effectief werken.

16. Bij het bepalen van de geschiktheid van de criteria, om de beschrijving van de serviceorganisatie van haar systeem te evalueren, dient de IT-auditor van de serviceorganisatie te bepalen of de criteria ten minste het volgende bevatten:
    (a) Of de beschrijving weergeeft op welke wijze het systeem van de serviceorganisatie is opgezet en geïmplementeerd, met inbegrip van, in voorkomend geval:
        (i) De soorten diensten die worden verleend, met inbegrip van, in voorkomend geval de verwerkte transactiestromen;
        (ii) De procedures, binnen zowel de informatie technologie als handmatige systemen, waardoor diensten worden verleend, met inbegrip van, in voorkomend geval, , procedures waardoor transacties worden geïnitieerd, vastgelegd, verwerkt, gecorrigeerd voor zover noodzakelijk en overgebracht naar de rapportages en overige informatie die voor gebruikersorganisaties is opgesteld;
        (iii) De daarmee verband houdende vastleggingen en ondersteunende informatie, met inbegrip van, in voorkomend geval, administratie, ondersteunende informatie en specifieke rekeningen die worden gebruikt om transacties te initiëren, vast te leggen, te verwerken en erover te rapporteren; dit omvat tevens het corrigeren van onjuiste informatie en op welke wijze informatie naar de rapporten wordt overgebracht en op welke wijze overige informatie voor gebruikersorganisaties is opgesteld;
        (iv) Op welke wijze het systeem van de serviceorganisatie significante gebeurtenissen en omstandigheden, anders dan de transacties, behandelt;
        (v) het proces dat wordt gehanteerd om rapportages en overige informatie voor gebruikersorganisaties op te stellen;
        (vi) De gespecificeerde interne beheersingsdoelstellingen en interne beheersingsmaatregelen om die doelstellingen te bereiken;
        (vii) Aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie beschouwd bij de opzet van de interne beheersingsmaatregelen; en
        (viii) Andere aspecten van de beheersingsomgeving van de entiteit, het risico-inschattingsproces, het informatiesysteem (inclusief daarmee verband houdende processen) en communicatie, de beheersingsactiviteiten en de monitoringsbeheersingsmaatregelen die relevant zijn voor de diensten die worden verleend.
    (b) In het geval van een type 2 rapport, over de vraag of de beschrijving relevante details bevat over wijzigingen aan het systeem van de serviceorganisatie gedurende de verslagperiode die door de beschrijving wordt omvat.
    (c) Of de beschrijving informatie weglaat of verkeerd voorstelt die relevant is voor de reikwijdte van het systeem van de serviceorganisatie dat wordt omschreven, terwijl erkend wordt dat de beschrijving is opgesteld om aan de algemene behoeftes van een brede groep gebruikers en hun accountants te voldoen en dat de beschrijving daarom niet ieder aspect van het systeem van de serviceorganisatie kan bevatten dat iedere individuele gebruikersorganisatie en haar accountant in diens bijzondere omgeving belangrijk kan achten.

17. Bij het bepalen van de geschiktheid van de criteria om de opzet van de interne beheersingsmaatregelen te evalueren, dient de IT-auditor van de serviceorganisatie te bepalen of de criteria ten minste de vraag bevatten of:

    (a) De serviceorganisatie de risico's heeft geïdentificeerd die het bereiken van de interne beheersingsdoelstellingen die in de beschrijving van haar systeem staan vermeld in gevaar brengen; en

    (b) De interne beheersingsmaatregelen die in die beschrijving zijn geïdentificeerd, indien zij werken zoals beschreven, een redelijke mate van zekerheid verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet verhinderen.

18. Bij het bepalen van de geschiktheid van de criteria om de werking van interne beheersingsmaatregelen te evalueren bij het verschaffen van een redelijke mate van zekerheid dat de vermelde interne beheersingsdoelstellingen die in de beschrijving zijn geïdentificeerd bereikt zullen worden, dient de IT-auditor van de serviceorganisatie te bepalen of de criteria ten minste de vraag bevatten of de interne beheersingsmaatregelen gedurende de gespecificeerde verslagperiode consistent zijn toegepast. Dit houdt onder meer in of er handmatige interne beheersingsmaatregelen zijn toegepast door personen die de geschikte competentie en bevoegdheid hebben. (Zie Par. A13, A14 en A15)

Materialiteit

19. Bij het plannen en het uitvoeren van de opdracht dient de IT-auditor van de serviceorganisatie de materialiteit met betrekking tot de getrouwe weergave van de beschrijving, de geschiktheid van de opzet van de interne beheersingsmaatregelen en, in het geval van een type 2 rapport, de werking van interne beheersingsmaatregelen in aanmerking te nemen. (Zie Par. A16, A17 en A18)

Het verwerven van inzicht in het systeem van de serviceorgansatie

20. De IT-auditor van de serviceorganisatie dient inzicht in het systeem van de serviceorganisatie te verkrijgen, met inbegrip van interne beheersingsmaatregelen die bij de reikwijdte van de opdracht zijn inbegrepen. (Zie Par. A19 en A20)

Het verkrijgen van assurance-informatie met betrekking tot de beschrijving

21. 3000ADe IT-auditor van de serviceorganisatie dient de beschrijving van de serviceorganisatie van haar systeem te verkrijgen en te lezen en dient te evalueren of die aspecten van de beschrijving die bij de reikwijdte van de opdracht zijn inbegrepen getrouw zijn weergegeven, met inbegrip van de vraag of: (Zie Par. A21 en A22)
    (a) De interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld in de gegeven omstandigheden redelijk zijn; (Zie Par. A23)
    (b) Interne beheersingsmaatregelen geïdentificeerd in de beschrijving, zijn geïmplementeerd;
    (c) Aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie, indien aanwezig, adequaat zijn beschreven; en
    (d) Diensten die door een subserviceorganisatie, indien aanwezig, zijn uitgevoerd adequaat zijn beschreven, met inbegrip van of de opname methode (inclusive methode) of de uitsluitingmethode (carve-out methode) is gehanteerd met betrekking tot die diensten.

22. De IT-auditor van de serviceorganisatie dient middels overige werkzaamheden in combinatie met verzoeken om inlichtingen te bepalen of het systeem van de serviceorganisatie is geïmplementeerd. Die overige werkzaamheden dienen observatie en inspectie van vastleggingen en overige documentatie te bevatten van de manier waarop het systeem van de serviceorganisatie werkt en interne beheersingsmaatregelen zijn toegepast. (Zie Par. A24)

Het verkrijgen van assurance-informatie met betrekking tot de opzet van interne beheersingsmaatregelen

23. De IT-auditor van de serviceorganisatie dient te bepalen welke van de interne beheersingsmaatregelen van de serviceorganisatie noodzakelijk zijn om de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld te bereiken en dient te beoordelen of die interne beheersingsmaatregelen op afdoende wijze zijn opgezet. De bepaling hiervan dient het volgende te bevatten: (Zie Par. A25, A26 en A27)
    (a) Het identificeren van de risico's die het bereiken van de interne beheersingsdoelstellingen die de beschrijving van de serviceorganisatie van haar systeem staan vermeld in gevaar brengen; en
    (b) Het evalueren van de koppeling van interne beheersingsmaatregelen geïdentificeerd in de beschrijving van de serviceorganisatie van haar systeem aan deze risico's.

Het verkrijgen van assurance-informatie met betrekking tot de werking van interne beheersingsmaatregelen

24. Wanneer een type 2 rapport wordt verstrekt dient de IT-auditor van de serviceorganisatie die interne beheersingsmaatregelen te toetsen waarvan de IT-auditor van de serviceorganisatie heeft bepaald dat zij noodzakelijk zijn om de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld te bereiken, en dient hij hun werking gedurende de verslagperiode vast te stellen. De assurance-informatie die in eerdere opdrachten is verkregen over de toereikende werking van interne beheersingsmaatregelen in eerdere verslagperiodes verschaft geen basis voor een vermindering van het toetsen**,** zelfs niet wanneer die is aangevuld met assurance-informatie die tijdens de lopende verslagperiode is verkregen. (Zie Par. A28-A32)

25. Bij het opzetten en het uitvoeren van de toetsing van interne beheersingsmaatregelen dient de IT-auditor van de serviceorganisatie:
    (a) Overige werkzaamheden uit te voeren in combinatie met verzoeken om inlichtingen om assurance-informatie te verkrijgen over:
        (i) Op welke wijze de interne beheersingsmaatregel was toegepast;
        (ii) De consistentie waarmee de interne beheersingsmaatregel was toegepast; en
        (iii) De vraag door wie of met welke middelen de interne beheersingsmaatregel is toegepast;
    (b) Vast te stellen of de te toetsen interne beheersingsmaatregelen afhankelijk zijn van andere interne beheersingsmaatregelen (indirecte interne beheersingsmaatregelen) en, zo ja, of het noodzakelijk is om assurance- informatie te verkrijgen die de werking van die indirecte interne beheersingsmaatregelen onderbouwt; en (Zie Par. A33 en A34)
    (c) Methodes te bepalen voor het selecteren van items ter toetsing die effectief zijn in het bereiken van de doelstellingen van de controlemaatregel. (Zie Par. A35 en A36)

26. Bij het bepalen van de omvang van de toetsing van interne beheersingsmaatregelen dient de IT-auditor van de serviceorganisatie aangelegenheden, met inbegrip van de kenmerken van de te toetsen populatie te overwegen, hetgeen omvat de aard van de interne beheersingsmaatregelen, de frequentie van hun toepassing (bijvoorbeeld maandelijks, dagelijks, een aantal keren per dag), en de verwachte mate van deviatie.

Het gebruiken van steekproeven

27. Wanneer de IT-auditor van de serviceorganisatie gebruik maakt van steekproeven dient de IT-auditor van de serviceorganisatie: (Zie Par. A35 en A36)
    (a) Het doel van de controlemaatregel en de kenmerken van de populatie van waaruit de steekproef zal worden genomen bij het opzetten van de steekproef te overwegen;
    (b) Een afdoende grootte van de steekproef te bepalen die het steekproefrisico tot een aanvaardbaar laag niveau verlaagt;
    (c) Items voor de steekproef te selecteren op een dergelijke manier dat iedere steekproefeenheid in de populatie een kans heeft om geselecteerd te worden;
    (d) Indien een opgezette controlemaatregel niet van toepassing is op het geselecteerde item, de controlemaatregel op een vervangend item uit te voeren; en
    (e) Indien hij niet in staat is om de opgezette werkzaamheden, of geschikte andere werkzaamheden, op een geselecteerd item toe te passen, dat item als een deviatie te behandelen.

Aard en oorzaak van deviaties

28. De IT-auditor van de serviceorganisatie dient de aard en de oorzaak van de onderkende deviaties te onderzoeken en dient te bepalen of:
    (a) Geïdentificeerde deviaties binnen de verwachte mate van deviatie en aanvaardbaar zijn; daarom verschaft de reeds uitgevoerde toetsing een geschikte basis om te concluderen dat de interne beheersingsmaatregel gedurende de gespecificeerde verslagperiode effectief werkt;
    (b) Aanvullende toetsing van de interne beheersingsmaatregel of overige interne beheersingsmaatregelen noodzakelijk is om tot een conclusie te komen dat de interne beheersingsmaatregelen met betrekking tot een bepaalde interne beheersingsdoelstelling gedurende de gespecificeerde verslagperiode effectief werken; of (Zie Par. A25)
    (c) De uitgevoerde toetsing een geschikte basis verschaft om te concluderen dat de interne beheersingsmaatregel gedurende de gespecificeerde verslagperiode niet effectief werkte.

29. In de zeer zeldzame gevallen waar de IT-auditor van de serviceorganisatie overweegt dat een ontdekte deviatie in een steekproef een a-typische fout is en er geen enkele andere interne beheersingsmaatregelen zijn onderkend die het voor de IT-auditor van de serviceorganisatie mogelijk maken te concluderen dat de relevante interne beheersingsdoelstelling gedurende de gespecificeerde verslagperiode wordt behaald, dient de IT-auditor van de serviceorganisatie een hoge mate van zekerheid te verkrijgen dat een dergelijk deviatie niet representatief is voor de populatie. De IT-auditor van de serviceorganisatie dient deze mate van zekerheid te verkrijgen door aanvullende werkzaamheden uit te voeren om voldoende en geschikte assurance- informatie te verkrijgen dat de deviatie geen invloed heeft op het resterende deel van de populatie.

De werkzaamheden van een interne auditfunctie[9]

Het verwerven van inzicht in de interne auditfunctie

30. Indien de serviceorganisatie een interne auditfunctie heeft, dient de IT-auditor van de serviceorganisatie een inzicht in de aard van de verantwoordelijkheden van de interne auditfunctie te verwerven alsmede in de werkzaamheden die worden uitgevoerd om te bepalen of het waarschijnlijk is dat de interne auditfunctie relevant is voor de opdracht. (Zie Par. A37)

Bepalen of en in welke mate van de werkzaamheden van de interne auditors gebruik kan worden gemaakt

31. De IT-auditor van de serviceorganisatie dient te bepalen:
    (a) Of het waarschijnlijk is dat de werkzaamheden van de interne auditors adequaat zijn voor de doeleinden van de opdracht; en
    (b) Zo ja, wat de geplande invloed is van de werkzaamheden van de interne auditors op de aard, de timing of omvang van de werkzaamheden van de IT-auditor van de serviceorganisatie.

32. Bij het bepalen of de werkzaamheden van de interne auditors waarschijnlijk adequaat zijn voor de doeleinden van de opdracht, dient de IT-auditor van de serviceorganisatie het volgende te evalueren:
    (a) De objectiviteit van de interne auditfunctie;
    (b) De technische competentie van de interne auditors;
    (c) Of de werkzaamheden van de interne auditors waarschijnlijk met voldoende professionele zorgvuldigheid worden uitgevoerd; en
    (d) Of het waarschijnlijk is dat er effectieve communicatie zal plaatsvinden tussen de interne auditors en de IT-auditor van de serviceorganisaties.

33. Bij het bepalen van de geplande invloed van de werkzaamheden van de interne auditors op de aard, timing of omvang van de werkzaamheden van de IT-auditor van de serviceorganisatie, dient de IT-auditor van de serviceorganisatie te overwegen: (Zie Par. A38)
    (a) De aard en de reikwijdte van de gespecificeerde werkzaamheden die door de interne auditors zijn uitgevoerd of uitgevoerd moeten worden;
    (b) De significantie van die werkzaamheden voor de conclusies van de IT-auditor van de serviceorganisatie; en
    (c) De mate van subjectiviteit die is gehanteerd bij de evaluatie van de assurance- informatie die ter ondersteuning van die conclusies is verzameld.

Gebruik maken van de werkzaamheden van de interne auditfunctie

34. Om gebruik te maken van specifieke werkzaamheden van de interne auditors, dient de IT-auditor van de serviceorganisatie die werkzaamheden te evalueren en daarop werkzaamheden uit te voeren om te bepalen of zij adequaat zijn voor de doeleinden van de IT-auditor van de serviceorganisatie. (Zie Par. A39)

35. Om het adequaat zijn van specifieke werkzaamheden die door de interne auditors zijn uitgevoerd voor de doeleinden van de IT-auditor van de serviceorganisatie te bepalen, dient de IT-auditor van de serviceorganisatie te evalueren of:
    (a) De werkzaamheden zijn uitgevoerd door interne auditors die beschikken over adequate vaktechnische training en vaardigheid;
    (b) Op de werkzaamheden naar behoren toezicht is uitgeoefend en of ze naar behoren werden beoordeeld en gedocumenteerd;
    (c) Adequate assurance- informatie is verkregen om de interne auditors in staat te stellen redelijke conclusies te trekken;
    (d) De bereikte conclusies onder de gegeven omstandigheden passend zijn en of alle rapportages opgesteld door de interne auditors consistent zijn met de uitkomsten van de uitgevoerde werkzaamheden; en
    (e) Uitzonderingen die voor de opdracht of ongebruikelijke aangelegenheden die door de interne auditors naar voren zijn gebracht naar behoren worden opgelost.

Effect op het assurance-rapport van de IT-auditor van de serviceorganisatie

[9] In deze Richtlijn worden geen situaties behandeld waarbij de interne IT-auditors directe assistentie verlenen aan de IT-auditor van de serviceorganisatie bij het uitvoeren van controlewerkzaamheden.

36. Indien er gebruik is gemaakt van de werkzaamheden van de interne auditfunctie dient de IT-auditor van de serviceorganisatie in de sectie van het assurance-rapport dat zijn oordeel bevat niet te verwijzen naar die werkzaamheden . (Zie Par. A40)

37. In het geval van een type 2 rapport, indien er gebruik is gemaakt van de werkzaamheden van de interne auditfunctie bij het toetsen van interne beheersingsmaatregelen, dient het onderdeel van het assurance-rapport van de IT-auditor van de serviceorganisatie, dat de toetsing door de IT-auditor van de serviceorganisatie van de interne beheersingsmaatregelen en de resultaten daarvan beschrijft, een beschrijving van het werk van de interne auditor en van de werkzaamheden van de IT-auditor van de serviceorganisatie met betrekking tot die werkzaamheden te bevatten. (Zie Par. A41)

Schriftelijke bevestigingen

38. De IT-auditor van de serviceorganisatie dient de serviceorganisatie te verzoeken om schriftelijke bevestigingen te verschaffen die: (Zie Par. 42)
    (a) De vermelding opnieuw bevestigen die samengaat met de beschrijving van het systeem;
    (b) Vermelden dat de serviceorganisatie alle relevante informatie en overeengekomen toegang aan de IT-auditor van de serviceorganisatie heeft verschaft[10]; en
    (c) Vermelden dat de serviceorganisatie de IT-auditor van de serviceorganisatie heeft ingelicht over de volgende zaken waarvan de serviceorganisatie op de hoogte is:
        (i) Het niet-naleven van wet- en regelgeving, fraude, ongecorrigeerde deviaties die toe te schrijven zijn aan de serviceorganisatie die één of meer gebruikersorganisaties kunnen beïnvloeden;
        (ii) Tekortkomingen in de opzet van interne beheersingsmaatregelen;
        (iii) Gevallen waarin interne beheersingsmaatregelen niet hebben gewerkt zoals stond beschreven; en
        (iv) Alle gebeurtenissen na de einddatum van de verslagperiode, die de beschrijving van de serviceorganisatie van haar systeem omvat tot aan de datum van het assurance-rapport van de IT-auditor van de serviceorganisatie, die een significantie invloed zouden kunnen hebben op het assurance-rapport van de IT-auditor van de serviceorganisatie.

39. De schriftelijke bevestigingen dienen in de vorm van een bevestigingsbrief geadresseerd aan de IT-auditor van de serviceorganisatie te zijn. De datum van de schriftelijke bevestigingen dient zo dicht als praktisch uitvoerbaar is bij, maar niet na, de datum van het assurance-rapport van de IT-auditor van de serviceorganisatie te liggen.

40. Indien, na de aangelegenheid met de IT-auditor van de serviceorganisatie te hebben besproken, de serviceorganisatie niet één of meerdere schriftelijke bevestigingen verschaft die in overeenstemming met paragraaf 38(a) en (b) van deze Standaard zijn verzocht, dient de IT-auditor van de serviceorganisatie een oordeelonthouding te formuleren. (Zie Par. A43)

Overige informatie

41. De IT-auditor van de serviceorganisatie dient de eventuele overige informatie te lezen die is inbegrepen bij een document dat de beschrijving van de serviceorganisatie van haar systeem en het assurance-rapport van de IT-auditor van de serviceorganisatie bevat, om eventuele met die beschrijving van materieel belang zijnde inconsistenties te identificeren. De IT-auditor van de serviceorganisatie kan tijdens het lezen van de overige informatie met als doel de van materieel belang zijnde inconsistenties te identificeren, kennis krijgen van een duidelijke afwijking van de feiten in die overige informatie.

42. Indien de IT-auditor van de serviceorganisatie een van materieel belang zijnde inconsistentie identificeert of zich bewust wordt van een duidelijke afwijking van de feiten, dient de IT-auditor van de serviceorganisatie de aangelegenheid met de serviceorganisatie te bespreken. Indien de IT-auditor van de serviceorganisatie concludeert dat er in de overige informatie een van materieel belang zijnde inconsistentie of een afwijking van de feiten bestaat waarvan de serviceorganisatie weigert deze te corrigeren, dient de IT-auditor van de serviceorganisatie verder passende actie te ondernemen. (Zie Par. A44 en A45)

Gebeurtenissen na de einddatum van de verslagperiode

43. De IT-auditor van de serviceorganisatie dient te verzoeken om inlichtingen of de serviceorganisatie op de hoogte is van gebeurtenissen na de einddatum van de verslagperiode die door de beschrijving van de serviceorganisatie van haar systeem is omvat tot aan de datum van het assurance-rapport van de IT-auditor van de serviceorganisatie die ertoe zouden kunnen leiden dat de IT-auditor van de serviceorganisatie het assurance-rapport aanpast. Indien de IT-auditor van de serviceorganisatie kennis heeft van een dergelijke gebeurtenis, en informatie over die gebeurtenis niet door de serviceorganisatie is toegelicht, dient de IT-auditor van de serviceorganisatie het in het assurance-rapport van de IT-auditor van de serviceorganisatie toe te lichten.

44. De IT-auditor van de serviceorganisatie heeft geen verplichting om werkzaamheden uit te voeren met betrekking tot de beschrijving van het systeem van de serviceorganisatie, of de geschiktheid van de opzet of de werking van de interne beheersingsmaatregelen, na de datum van het assurance-rapport van de IT-auditor van de serviceorganisatie.

Documentatie

45. De IT-auditor van de serviceorganisatie dient tijdig opdrachtdocumentatie op te stellen die een vastlegging verschaft van de basis voor het assurance-rapport die voldoende en geschikt is om een ervaren IT-auditor van een serviceorganisatie die voorheen niet bij de opdracht betrokken was, in staat te stellen inzicht te verwerven in:
   (a) De aard, timing en omvang van de werkzaamheden die zijn uitgevoerd overeenkomstig deze Richtlijn en in overeenstemming met de van toepassing zijnde door wet- en regelgeving gestelde eisen;
   (b) De uitkomsten van de uitgevoerde werkzaamheden en de verkregen assurance- informatie; en
   (c) Significante aangelegenheden voortgekomen uit de opdracht, de daaruit getrokken conclusies en significante professionele oordelen die zijn gevormd om tot die conclusies te komen.

46. Bij het documenteren van de aard, timing en omvang van de uitgevoerde werkzaamheden dient de IT-auditor het volgende vast te leggen:
   (a) De onderscheidende kenmerken van de specifieke items of aangelegenheden die worden getoetst;
   (b) Wie de werkzaamheden heeft uitgevoerd en de datum waarop dergelijke werkzaamheden zijn voltooid; en
   (c) Wie de werkzaamheden heeft beoordeeld en de datum en omvang van een dergelijke beoordeling.

47. Indien de IT-auditor van de serviceorganisatie gebruik maakt van de werkzaamheden van de interne IT-auditors, dient de IT-auditor van de serviceorganisatie de conclusies die getrokken zijn met betrekking tot de evaluatie van het adequaat zijn van de werkzaamheden van de interne IT-auditors, en de door de IT-auditor van de serviceorganisaties uitgevoerde werkzaamheden met betrekking tot die werkzaamheden,

[10] Paragraaf 13(b)(v) van deze Richtlijn.

te documenteren.

48. De IT-auditor van de serviceorganisatie dient de besprekingen met de serviceorganisatie en overigen over significante aangelegenheden te documenteren met inbegrip van de aard van de besproken significante aangelegenheden en wanneer en met wie deze besprekingen plaatsvonden.

49. Indien de IT-auditor van de serviceorganisatie informatie heeft geïdentificeerd die inconsistent is met de uiteindelijke conclusie van de IT-auditor van de serviceorganisatie met betrekking tot een significante aangelegenheid, dient de IT-auditor van de serviceorganisatie te documenteren op welke wijze de IT-auditor van de serviceorganisatie de inconsistentie heeft behandeld.

50. De IT-auditor van de serviceorganisatie dient de documentatie in een opdrachtdossier samen te stellen en het administratieve proces van samenstelling van het definitieve dossier tijdig na de datum van zijn assurance-rapport te voltooien[11].

51. Nadat het samenstellen van het definitieve opdrachtdossier is voltooid, dient de IT-auditor van de serviceorganisatie geen documentatie te vernietigen of te verwijderen voordat de bewaarperiode is afgelopen. (Zie Par. A46)

52. Indien de IT-auditor van de serviceorganisatie het noodzakelijk acht om bestaande opdrachtdocumentatie aan te passen of nieuwe documentatie nadat de samenstelling van het definitieve opdrachtdossier is voltooid, toe te voegen en die documentatie geen invloed heeft op de rapportage van de IT-auditor van de serviceorganisatie, dient de IT-auditor van de serviceorganisatie, ongeacht de aard van de aanpassingen of de toevoegingen, het volgende te documenteren:
   (a) De specifieke redenen voor het aanbrengen daarvan; en
   (b) Wanneer en door wie ze werden aangebracht en beoordeeld.

Het opstellen van het assurance-rapport van de IT-auditor van de serviceorganisatie

De inhoud van het assurance-rapport van de IT-auditor van de serviceorganisatie

53. Het assurance-rapport van de IT-auditor van de serviceorganisatie dient minstens de volgende basiselementen te bevatten: (Zie Par. A47)
   (a) Een titel die duidelijk aangeeft dat de rapportage een assurance-rapport is van een onafhankelijke IT-auditor.
   (b) Een geadresseerde.
   (c) Het aanduiden van:
      (i) De beschrijving van de serviceorganisatie van haar systeem en de vermelding van de serviceorganisatie die de aangelegenheden bevatten die beschreven zijn in paragraaf 9(k)(ii) voor een type 2 rapport, of paragraaf 9(j)(ii) voor een type 1 rapport.
      (ii) De eventuele onderdelen van de beschrijving van de serviceorganisatie van haar systeem die niet door het oordeel van de IT-auditor van de serviceorganisatie worden omvat.
      (iii) Indien de beschrijving naar de behoefte aan aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie verwijst, een vermelding dat de IT-auditor van de serviceorganisatie de geschiktheid van de opzet of de werking van aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie niet heeft geëvalueerd, en dat de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld alleen maar kunnen worden bereikt, indien de aanvullende interne beheersingsmaatregelen van een gebruikersorganisatie samen met de interne beheersingsmaatregelen van de serviceorganisatie op afdoende wijze zijn opgezet of werken.

(iv) Indien diensten door een subserviceorganisatie worden uitgevoerd, de aard van de activiteiten die door de subserviceorganisatie worden uitgevoerd zoals die staan beschreven in de beschrijving van de serviceorganisatie van haar systeem en of er van de opname methode (inclusive methode) of de uitsluitingmethode (carve-out methode) met betrekking tot die diensten gebruik is gemaakt. Waar er van de uitsluitingmethode (carve-out methode) gebruik is gemaakt, een vermelding dat de beschrijving van de serviceorganisatie van haar systeem de interne beheersingsdoelstellingen en daarmee verband houdende interne beheersingsmaatregelen van relevante subserviceorganisaties uitsluit en dat werkzaamheden van de IT-auditor van de serviceorganisatie zich niet uitstrekken tot de interne beheersingsmaatregelen van de subserviceorganisatie. Waar er gebruik is gemaakt van de opname methode (inclusive methode), een vermelding dat de beschrijving van de subserviceorganisatie van haar systeem de interne beheersingsdoelstellingen en de daarmee verband houdende interne beheersingsmaatregelen van de serviceorganisatie omvat, en dat de werkzaamheden van de IT-auditor van de serviceorganisatie zich uitstrekten tot de interne beheersingsmaatregelen van de subserviceorganisatie.

(d) Aanduiding van de van toepassing zijnde criteria en de partij die de interne beheersingsdoelstellingen specificeert.

(e) Een vermelding dat de rapportage en, in het geval van een type 2 rapport, de beschrijving van toetsingen van interne beheersingsmaatregelen alleen voor gebruikersorganisaties en hun accountants, die afdoende inzicht hebben om deze te beschouwen zijn bedoeld, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door gebruikersorganisaties zelf worden uitgevoerd, wanneer zij de risico's op afwijkingen van materieel belang in de financiële overzichten van gebruikersorganisaties inschatten. (Zie Par. A48)

(f) Een vermelding dat de serviceorganisatie verantwoordelijk is voor:

(i) Het opstellen van de beschrijving van haar systeem en de bijgaande vermelding, met inbegrip van de volledigheid, nauwkeurigheid en de methode van presentatie van die beschrijving en die vermelding;

(ii) Het verlenen van de diensten die door de beschrijving van de serviceorganisatie van haar systeem wordt omvat;

(iii) het vermelden van de interne beheersingsdoelstellingen (waar zij niet zijn geïdentificeerd door wet- of regelgeving, of een andere partij bijvoorbeeld een gebruikersgroep of een beroepsorganisatie); en

(iv) Het opzetten en implementeren van interne beheersingsmaatregelen om de interne beheersingsdoelstellingen te bereiken die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld.

(g) Een vermelding dat de verantwoordelijkheid van de IT-auditor van de serviceorganisatie ligt bij het tot uitdrukking brengen van een oordeel over de beschrijving van de serviceorganisatie, over de opzet van interne beheersingsmaatregelen die verband houden met interne beheersingsdoelstellingen die in die beschrijving staan vermeld, en, in het geval van een type 2 rapport, over de werking van die interne beheersingsmaatregelen op basis van de werkzaamheden van de IT-auditor van de serviceorganisatie.

(h) Een vermelding dat de IT-auditeenheid waarbij de IT-auditor werkzaam is of aan verbonden is, het Reglement Kwaliteitsbeheersing NOREA (RKBN) of andere wettelijke of professionele vereisten die tenminste gelijkwaardig is toepast. Indien de opdrachtpartner geen IT-auditor is, dient de vermelding de vergelijkbare professionele vereisten te identificeren, die zijn toegepast.

(i) Een vermelding dat de IT-auditor de vereisten van het Reglement Gedragscode ('Code of Ethics') heeft nageleefd. Als de opdracht partner geen IT-auditor is, dient de vermelding de professionele vereisten die tenminste gelijkwaardig zijn te identificeren die zijn toegepast.

(j) Een vermelding dat de opdracht overeenkomstig Richtlijn 3402 "Assurance-rapporten betreffende interne

[11] Een geschikt tijdsbestek waarbinnen de samenstelling van het definitieve opdracht-dossier moet worden afgerond, is gewoonlijk niet meer dan 60 dagen na de datum van het assurance-rapport (zie Richtlijn 230, paragraaf A21)).

beheersingsmaatregelen bij een serviceorganisatie" is uitgevoerd, op grond waarvan van de IT-auditor wordt vereist dat hij de werkzaamheden uitvoert om een redelijke mate van zekerheid te verkrijgen of, in alle van materieel belang zijnde opzichten, de beschrijving van de serviceorganisatie van haar systeem een getrouwe weergave is en de interne beheersingsmaatregelen op afdoende wijze zijn opgezet en, in het geval van een type 2 rapport, effectief werken.

(k) Een samenvatting van de werkzaamheden van de IT-auditor van de serviceorganisatie om een redelijke mate van zekerheid te verkrijgen en een vermelding dat de IT-auditor van mening is dat de verkregen assurance- informatie voldoende en geschikt is om een basis voor het oordeel van de IT-auditor van de serviceorganisatie te verschaffen en, in het geval van een type 1 rapport, een vermelding dat de IT-auditor van de serviceorganisatie geen werkzaamheden met betrekking tot de werking van interne beheersingsmaatregelen heeft uitgevoerd en er daarom daarover geen oordeel r tot uitdrukking wordt gebracht.

(l) Een vermelding van de beperkingen van interne beheersingsmaatregelen en, in het geval van een type 2 rapport, van het risico van het projecteren naar toekomstige verslagperiodes van een evaluatie betreffende de werking van interne beheersingsmaatregelen.

(m) Het oordeel van de IT-auditor van de serviceorganisatie, dat in de positieve vorm tot uitdrukking is gebracht, over of, in alle van materieel belang zijnde opzichten, op basis van geschikte criteria:

a. In het geval van een type 2 rapport:
   i. De beschrijving het systeem van de serviceorganisatie, dat gedurende de gespecificeerde verslagperiode is opgezet en geïmplementeerd, getrouw weergeeft;
   ii. De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, gedurende de gespecificeerde verslagperiode op afdoende wijze zijn opgezet; en
   iii. De getoetste interne beheersingsmaatregelen, die noodzakelijk waren om een redelijke mate van zekerheid te verschaffen dat de interne beheersingsdoelstellingen die in de beschrijving staan vermeld,, zijn bereikt gedurende de gespecificeerde verslagperiode effectief werkten.

b. In het geval van een type 1 rapport:
   i. De beschrijving het systeem van de serviceorganisatie, dat op de gespecificeerde datum is opgezet en geïmplementeerd, getrouw weergeeft;
   ii. De interne beheersingsmaatregelen die betrekking hebben op de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem vermeld staat, op de gespecificeerde datum op afdoende wijze zijn opgezet.

(n) De datum van het assurance-rapport van de IT-auditor van de serviceorganisatie, die niet eerder zal zijn dan de datum waarop de IT-auditor van de serviceorganisatie de assurance-informatie heeft verkregen waarop zijn oordeel is gebaseerd.

(o) De naam van de IT-auditor van de serviceorganisatie en de locatie in het rechtsgebied waarin de IT-auditor van de serviceorganisatie werkzaam is.

54. In het geval van een type 2 rapport dient het assurance-rapport van de IT-auditor van de serviceorganisatie een separate sectie na het oordeel, of een bijlage, te bevatten die de uitgevoerde toetsingen van de interne beheersingsmaatregelen en de resultaten daarvan beschrijft. Bij het beschrijven van die toetsingen dient de IT-auditor van de serviceorganisatie duidelijk te vermelden welke interne beheersingsmaatregelen zijn getoetst, aan te duiden of de getoetste elementen alle of een selectie van de elementen in de populatie weergeven en de aard van de getoetste elementen op afdoende gedetailleerde wijze aan te geven om de gebruikende accountant in staat te stellen de invloed van dergelijke toetsingen op hun risico-inschattingen te bepalen. Indien er deviaties zijn geïdentificeerd, dient de IT-auditor van de serviceorganisatie de omvang van de uitgevoerde toetsen die leidde naar het identificeren van de deviaties, erbij te betrekken (met inbegrip van de grootte van de steekproef waar er van een steekproef gebruik werd gemaakt), en het aantal en de aard van de geconstateerde deviaties. De IT-auditor van de serviceorganisatie dient deviaties te rapporteren zelfs als, op basis van de uitgevoerde toetsingen, de IT-auditor van de serviceorganisatie geconcludeerd heeft dat de gerelateerde beheersingsdoelstelling was bereikt. (Zie Par. A18 en A49)

Aangepaste oordelen

55. Indien de IT-auditor van de serviceorganisatie concludeert dat: (Zie Par. A50, A51 en A52)

(a) De beschrijving van de serviceorganisatie het systeem, zoals dit is opgezet en geïmplementeerd, in alle van materieel belang zijnde aspecten, niet getrouw weergeeft;

(b) De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld, niet op afdoende wijze zijn opgezet, in alle van materieel belang zijnde opzichten;

(c) In het geval van een type 2 rapport de getoetste interne beheersingsmaatregelen, die noodzakelijk waren om een redelijke mate van zekerheid te verschaffen dat de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie staan vermeld, zijn bereikt, in alle van materieel belang zijnde opzichten, niet effectief werkten; of

(d) De IT-auditor van de serviceorganisatie niet in staat is om voldoende en geschikte assurance- informatie te verkrijgen, dient het oordeel van de IT-auditor van de serviceorganisatie te worden aangepast en dient het assurance-rapport van de IT-auditor van de serviceorganisatie een sectie te bevatten met een duidelijke beschrijving van alle redenen voor die aanpassing.

Overige communicatieverantwoordelijkheden

56. Indien de IT-auditor van de serviceorganisatie kennis krijgt van het niet-naleven van wet-en regelgeving, fraude of niet-gecorrigeerde fouten die toe te schrijven zijn aan de serviceorganisatie en die niet duidelijk triviaal zijn en een of meerdere gebruikersorganisaties kunnen beïnvloeden, dient de IT-auditor van de serviceorganisatie te bepalen of de aangelegenheid op de geschikte wijze is gecommuniceerd aan de getroffen gebruikersorganisaties. Indien de aangelegenheid niet op die manier is besproken en de serviceorganisatie niet bereid is om dat te doen, dient de IT-auditor van de serviceorganisatie passende actie te ondernemen. (Zie Par. A53)

Toepassingsgerichte en overige verklarende teksten

Toepassingsgebied van deze Richtlijn (Zie Par. 1 en 3)

A1. Interne beheersing is een proces dat is opgezet om een redelijke mate van zekerheid te verschaffen betreffende het bereiken van de doelstellingen die verband houden met de betrouwbaarheid van de financiële verslaggeving, de effectiviteit en efficiency van activiteiten en het naleven van toepasselijke wet- en regelgeving. Interne beheersingsmaatregelen met betrekking tot doelstellingen met betrekking tot de activiteiten en het naleven van wet- en regelgeving van een serviceorganisatie kunnen relevant zijn voor de interne beheersing van een gebruikersorganisatie in relatie tot de financiële verslaggeving. Dergelijke interne beheersingsmaatregelen maken deel uit van de beweringen betreffende de presentatie en toelichting met betrekking tot saldi, transactiestromen of toelichtingen, of zij maken deel uit van assurance- informatie die de gebruikende accountant evalueert of hier gebruik van maakt bij het toepassen van de controlewerkzaamheden. De interne beheersingsmaatregelen, bijvoorbeeld, van een serviceorganisatie die de loonkosten verwerkt, die betrekking hebben op het tijdig afdragen van de wettelijke inhoudingen op het loon aan overheidsautoriteiten zijn mogelijk relevant voor een gebruikersorganisatie aangezien late afdrachten op rente en boetes kunnen uitlopen die voor een gebruikersorganisatie zouden resulteren in een schuld. Op vergelijkbare wijze worden de interne beheersingsmaatregelen betreffende de aanvaardbaarheid van investeringstransacties vanuit een regelgevend perspectief mogelijk gezien als relevant voor de presentatie en toelichting van de transacties en rekeningsaldi van een gebruikersorganisatie in haar financiële overzichten. De bepaling of de interne beheersingsmaatregelen bij een serviceorganisatie die verband houden met activiteiten en naleving waarschijnlijk relevant zijn voor de interne beheersing van gebruikersorganisaties in relatie tot de financiële verslaggeving is een aangelegenheid van professionele oordeelsvorming, waarbij de interne beheersingsdoelstellingen die door de

	serviceorganisatie zijn opgezet en de geschiktheid van de criteria in acht moeten worden genomen.
A2.	De serviceorganisatie kan niet in staat zijn om te beweren dat het systeem op afdoende wijze is opgezet wanneer, bijvoorbeeld, de serviceorganisatie met een systeem werkt dat door een gebruikersorganisatie is opgezet of in een contract tussen de gebruikersorganisatie en de serviceorganisatie is vastgelegd. Vanwege de onlosmakelijke verbinding tussen de geschikte opzet van de interne beheersingsmaatregelen en hun werking, zal het ontbreken van een vermelding met betrekking tot de geschiktheid van de opzet de IT-auditor van de serviceorganisatie waarschijnlijk beletten te concluderen dat de interne beheersingsmaatregelen een redelijke mate van zekerheid verschaffen dat de interne beheersingsdoelstellingen zijn bereikt en bijgevolg de IT-auditor van de serviceorganisatie beletten te oordelen over de werking van interne beheersingsmaatregelen. Als andere mogelijkheid kan de IT-auditor ervoor kiezen een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden te aanvaarden om de toetsingen van interne beheersingsmaatregelen of een assurance-opdracht op basis van Richtlijn 3000A uit te voeren om te kunnen concluderen of, op basis van toetsingen van interne beheersingsmaatregelen, de interne beheersingsmaatregelen werken zoals staat beschreven.
Definities (Zie Par. 9(d) en 9(g))	
A3.	De definitie van "interne beheersingsmaatregelen bij een serviceorganisatie" omvat aspecten van informatiesystemen van gebruikersorganisaties die door de serviceorganisatie zijn onderhouden en kunnen ook aspecten van een of meer van de componenten van interne beheersing van een serviceorganisatie bevatten. Het kan bijvoorbeeld aspecten bevatten van de beheersingsomgeving, het monitoren en beheersingsactiviteiten van een serviceorganisatie wanneer deze verband houden met de verleende diensten. Het bevat echter geen interne beheersingsmaatregelen van een serviceorganisatie die geen verband houden met het bereiken van de beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, zoals interne beheersingsmaatregelen die verband houden met het opstellen van de financiële overzichten van de serviceorganisatie zelf.
A4.	Wanneer er van de opname methode (inclusive methode) gebruik wordt gemaakt, zijn de vereisten in deze Richtlijn ook van toepassing op de diensten die door de subserviceorganisatie worden verleend, met inbegrip van het verkrijgen van overeenstemming met betrekking tot de aangelegenheden in paragraaf 13 (b)(i)-(v) zoals die op de subserviceorganisatie in plaats van de serviceorganisatie zijn toegepast. Het uitvoeren van werkzaamheden bij de subserviceorganisatie leidt tot coördinatie en communicatie tussen de serviceorganisatie, de subserviceorganisatie en de IT-auditor van de serviceorganisatie. De opname methode (inclusive methode) is doorgaans alleen haalbaar indien de serviceorganisatie en de subserviceorganisatie met elkaar zijn verbonden of als het contract tussen de serviceorganisatie en de subserviceorganisatie hierin voorziet.
Ethische voorschriften (Zie Par. 11)	
A5.	De IT-auditor van de serviceorganisatie is onderhevig aan de relevante onafhankelijkheidsvereisten zoals opgenomen in het Reglement Gedragscode ('Code of Ethics'). Bij het uitvoeren van een opdracht overeenkomstig deze Richtlijn wordt op grond van het Reglement Gedragscode niet van de IT-auditor van de serviceorganisatie vereist dat hij onafhankelijk is van elke gebruikersorganisatie.
Management en de met governance belaste personen (Zie Par. 12)	
A6.	De beheers- en goverancestructuren lopen per rechtsgebied en per entiteit uiteen, waardoor ze invloeden zoals verschillende culturele en juridische achtergronden en kenmerken van grootte en eigendom weerspiegelen. Een dergelijke verscheidenheid houdt in dat het voor deze Richtlijn niet mogelijk is om voor alle opdrachten de personen te specificeren met wie de IT-auditor van de serviceorganisatie in interactie moet staan met betrekking tot bepaalde aangelegenheden. De serviceorganisatie kan bijvoorbeeld een segment zijn van een derde organisatie en geen gescheiden juridische entiteit. In dergelijke gevallen is het mogelijk dat voor het identificeren van geschikt managementpersoneel of de met governance belaste personen bij wie de schriftelijke bevestigingen moeten worden verzocht, het toepassen van professionele oordeelsvorming is vereist.
Aanvaarding en continuering	
Capaciteiten en competentie om de opdracht uit te kunnen voeren (Zie Par. 13(a)(i))	
A7.	Relevante capaciteiten en competentie om de opdracht uit te voeren bevatten onder meer de volgende aangelegenheden: • Kennis van de betreffende sector; • Inzicht in informatietechnologie en systemen;
	• Ervaring met het evalueren van risico's aangezien deze verband houden met de geschikte opzet van interne beheersingsmaatregelen; en • Ervaring met het opzetten en het uitvoeren van toetsingen van interne beheersingsmaatregelen en met het evalueren van de resultaten.
De vermelding van een serviceorganisatie (Zie Par. 13(b)(i))	
A8.	De weigering door een serviceorganisatie om een schriftelijke vermelding te verschaffen, volgende op een overeenkomst van de IT-auditor van de serviceorganisatie om een opdracht te aanvaarden of te continueren, geeft een beperking in reikwijdte aan die ertoe leidt dat de IT-auditor van de serviceorganisatie de opdracht teruggeeft. Indien wet- of regelgeving de IT-auditor van de serviceorganisatie niet toestaat de opdracht terug te geven, formuleert de IT-auditor van de serviceorganisatie een oordeelonthouding.
Een redelijke basis voor de bewering van de serviceorganisatie (Zie Par. 13(b)(i))	
A9.	In het geval van een type 2 rapport, houdt de vermelding van de serviceorganisatie onder meer een vermelding in dat de interne beheersingsmaatregelen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld gedurende de gespecificeerde verslagperiode effectief werkten. Deze vermelding kan gebaseerd zijn op de monitoringactiviteiten van de serviceorganisatie. Het monitoren van interne beheersingsmaatregelen is een proces om de effectiviteit van interne beheersingsmaatregelen in de loop van de tijd vast te stellen. Het houdt onder meer het tijdig bepalen van de effectiviteit van de interne beheersingsmaatregelen in, het identificeren en rapporteren van tekortkomingen aan geschikte personen binnen de serviceorganisatie en het nemen van de noodzakelijke corrigerende acties. De serviceorganisatie brengt het monitoren van interne beheersingsmaatregelen tot stand middels voortdurende activiteiten, separate evaluaties of een combinatie van beiden. Hoe groter de mate van effectiviteit van voortdurende monitoringactiviteiten, des te kleiner de behoefte aan separate evaluaties. Voortdurende monitoringactiviteiten zijn vaak opgenomen in de normale terugkerende activiteiten van een serviceorganisatie en bevatten regelmatige leidinggevende en toezichthoudende activiteiten. Interne auditors of personeelsleden die vergelijkbare functies bekleden kunnen een bijdrage leveren aan het monitoren van de activiteiten van de serviceorganisatie. Monitoringactiviteiten kunnen ook het gebruik maken van informatie die door externe partijen wordt gecommuniceerd, inhouden, zoals klachten van cliënten en commentaar van regelgevers of toezichthouders die mogelijk op problemen wijzen of de nadruk leggen op gebieden die behoefte hebben aan verbetering. Het feit dat de IT-auditor van de serviceorganisatie over de werking van interne beheersingsmaatregelen zal rapporteren, is geen vervanging voor de processen van de serviceorganisatie zelf om een redelijke basis voor haar vermelding te verschaffen.
Het identificeren van risico's (Zie Par. 13(b)(iv))	
A10.	Zoals staat vermeld in paragraaf 9(c), houden interne beheersingsdoelstellingen verband met risico's waar de interne beheersingsmaatregelen ernaar streven deze te mitigeren. Het risico dat een transactie bijvoorbeeld op het verkeerde bedrag of in de verkeerde verslagperiode wordt vastgelegd kan als een interne beheersingsdoelstelling tot uitdrukking worden gebracht dat transacties op het juiste bedrag en in de juiste verslagperiode worden vastgelegd. De serviceorganisatie is verantwoordelijk voor het identificeren van de risico's die het bereiken van de interne beheersingsdoelstellingen die in de beschrijving van haar systeem staan vermeld in gevaar brengen. De serviceorganisatie kan een formeel of informeel proces hebben om relevante risico's te

identificeren. Een formeel proces kan het inschatten van de significantie van onderkende risico's inhouden, het inschatten van de waarschijnlijkheid dat zij zullen voorkomen en het besluiten welke acties moeten worden ondernomen om op die risico's in te spelen. Daar de interne beheersingsdoelstellingen echter verband houden met risico's waar interne beheersingsmaatregelen naar streven deze te mitigeren, kan weldoordachte identificatie van interne beheersingsdoelstellingen bij het opzetten en implementeren het systeem van de serviceorganisatie zelf bestaan uit een informeel proces voor het identificeren van relevante risico's.

Aanvaarding van een wijziging in de voorwaarden van de opdracht (Zie Par. 14)

A11. Een verzoek tot het wijzigen van de reikwijdte van de opdracht heeft mogelijk geen redelijke rechtvaardiging wanneer het verzoek bijvoorbeeld is gedaan om bepaalde interne beheersingsdoelstellingen uit te sluiten van de reikwijdte van de opdracht vanwege de waarschijnlijkheid dat het oordeel van de IT-auditor van de serviceorganisatie aangepast zou worden; of de serviceorganisatie zal de IT-auditor geen schriftelijke vermelding verschaffen en het verzoek wordt gedaan om de opdracht onder Richtlijn 3000A uit te voeren.

A12. Een verzoek tot het wijzigen van de reikwijdte van de opdracht kan een redelijke rechtvaardiging hebben wanneer het verzoek bijvoorbeeld is gedaan om een subserviceorganisatie van de opdracht uit te sluiten wanneer de serviceorganisatie geen toegang voor de IT-auditor van de serviceorganisatie kan regelen, en de methode waarvan gebruik wordt gemaakt bij het behandelen van de diensten die door die subserviceorganisatie worden verleend is gewijzigd van de opname methode (inclusive methode) naar de uitsluitingmethode (carve-out methode).

Het beoordelen van de geschiktheid van de criteria (Zie Par. 15 -18)

A13. Het is nodig dat criteria voor de beoogde gebruikers beschikbaar zijn om het hen mogelijk te maken inzicht te verkrijgen in de basis voor de vermelding van de serviceorganisatie betreffende de getrouwe weergave van haar systeem, de geschiktheid van het opzetten van interne beheersingsmaatregelen en, in het geval van een type 2 rapport, de werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen.

A14. Op grond van Richtlijn 3000A wordt er van de IT-auditor vereist dat hij, onder andere, bepaalt of de criteria die gebruikt worden geschikt zijn en de toepasselijkheid van het object van onderzoek bepaalt. Het object van onderzoek is de onderliggende conditie van belang voor de beoogde gebruikers van een assurance-rapport. De volgende tabel identificeert het object van onderzoek en minimale criteria voor elk van de oordelen in type 1 en type 2 rapporten.

	Object van onderzoek	**Criteria**	**Commentaar**
Oordeel over de getrouwe weergave van de beschrijving van de service-organisatie van haar systeem (type 1 en type 2 rapporten)	Het systeem van de service-organisatie dat waarschijnlijk relevant is voor de interne beheersing van de gebruikersorganisatie in relatie tot de financiële verslaggeving en door het assurance-rapport van de IT-auditor van de service-organisatie wordt omvat.	De beschrijving is een getrouwe weergave indien zij: (a) weergeeft op welke wijze het systeem van de serviceorganisatie is opgezet en geïmplementeerd, met inbegrip van, in voorkomend geval, de aangelegenheden die in paragraaf 16(a)(i)-(viii) zijn geïdentificeerd; (b), in het geval van een type 2 rapport, de relevante details van wijzigingen in het systeem van de serviceorganisatie omvat gedurende de verslagperiode die door de beschrijving wordt omvat bevat; en (c) voor de reikwijdte van het systeem van de serviceorganisatie dat is beschreven relevante informatie niet weglaat of verkeerd voorstelt, terwijl erkend wordt dat de beschrijving is opgesteld om aan de algemene behoeftes van een brede groep gebruikersorganisaties te voldoen en daarom niet ieder aspect van het systeem van de serviceorganisatie kan bevatten dat iedere individuele gebruikersorganisatie in diens eigen bijzondere omgeving belangrijk kan achten.	Het kan nodig zijn dat de specifieke bewoording van de criteria voor dit oordeel op maat wordt gesneden om con-sistent te zijn met de criteria die bijvoorbeeld door wet- of regelgeving, gebruikersgroepen of een beroepsorganisatie zijn opgesteld. Voorbeelden van criteria voor dit oordeel worden in de voorbeeld bewering van de serviceorganisatie in bijlage 1 ver-schaft. Paragraaf A21 tot en A24 verschaffen ver-dere leidraden bij het bepalen of er aan deze criteria wordt voldaan. (Aangaande de vereisten van Richtlijn 3000A, betreft de informatie[13] over het object van onderzoek voor dit oordeel de beschrijving van de serviceorganisatie van haar systeem en de bewering van de service-organisatie dat de beschrijving ge-trouw is weergegeven.)

[12] Richtlijn 3000A, paragraaf 24(b) en 41.

Oordeel over de geschiktheid van de opzet en de werking (type 2 rapporten)	De geschiktheid van de opzet en werking van de interne beheersings-maatregelen die noodzakelijk zijn om de beheersings-doelstellingen te bereiken die in de beschrijving van de service-organisatie staan vermeld.	De interne beheersingsmaatre-gelen zijn op afdoende wijze opgezet en werken effectief indien: (a) de serviceorganisatie de risico's die het bereiken van de beheer-singsdoelstellingen die in de beschrijving van haar systeem staan vermeld heeft benoemd; (b) de geïdentificeerde interne beheersingsmaatregelen die in die beschrijving, indien ze werken zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde beheersingsdoel-stellingen niet verhinderen; en (c) de interne beheersings-maatregelen consistent zijn toegepast zoals ze gedurende de ge-specificeerde ver-slagperiode zijn opgezet. Dit houdt in of handmatige interne beheersingsmaatregelen zijn toegepast door personen die de geschikte competentie en bevoegdheid hebben.	Wanneer er aan de criteria voor dit oordeel is voldaan, hebben de interne beheersings-maatregelen een redelijke mate van zekerheid verschaft dat de verbonden beheersings-doelstellingen gedurende de gespecificeerde verslagperiode zijn bereikt. (aangaande de vereisten van Richtlijn 3000A, betreft de informatie over het object van onderzoek voor dit oordeel de bewering van de service-organisatie dat de interne beheersingsmaat-regelen op af-doende wijze zijn opgezet en dat zij effectief werken.	De beheersings-doelstellingen, die in de beschrijving van de service-organisatie van haar systeem staan vermeld, zijn onderdeel van de criteria voor deze oordelen. De vermelde beheersings-doelstellingen zullen per opdracht verschillen. Indien, als onderdeel van het vormen van het oordeel over de beschrijving, de IT-auditor van de service-organisatie concludeert dat de vermelde beheersings-doelstellingen niet getrouw zijn weergegeven, zouden die beheersings-doelstellingen niet geschikt zijn als onderdeel van de criteria voor het vormen van een oordeel over de opzet of de doeltreffende werking van interne beheersings-maatregelen.
Oordeel over de geschikt-heid van de opzet (type 1 rapporten)	De geschiktheid van de opzet van die interne beheersings-maatregelen die noodzakelijk zijn om de beheer-singsdoelstellinge n die in de beschrij-ving van de ser-	De interne beheersings-maatregelen zijn op afdoende wijze opgezet indien: (a) de serviceorganisatie de risico's die het bereiken van de beheersingsdoelstel-lingen die in de beschrijving van haar systeem staan vermeld heeft geïdentificeerd; en (b) de interne beheer-singsmaatregelen die in die	Het voldoen aan deze criteria ver-schaft niet uit zich zelf enige zekerheid dat de verbonden beheersingsmaat-regelen zijn be-reikt omdat er geen enkele ze-kerheid over de werking van interne beheer-	

[13] De informatie over het object van onderzoek is de uitkomst van de evaluatie of meting van het object van onderzoek dat het resultaat is van het toepassen van de criteria op het object van onderzoek.

viceorganisatie van haar systeem zijn vermeld te bereiken.	geïdentificeerd, indien ze werken zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's niet verhinderen dat de vermelde beheersings-doelstellingen worden bereikt.	singsmaatregelen is verkregen. (Aangaande de vereisten van Richtlijn 3000A, betreft de informatie over het object van onderzoek voor dit oordeel de bewering van de serviceorganisatie dat de interne beheersingsmaat-regelen op af-doende wijze zijn opgezet.)	

A15. Paragraaf 16(a) identificeert een aantal elementen die in voorkomend geval bij de beschrijving van de serviceorganisatie van haar systeem zijn inbegrepen. Deze elementen kunnen niet geschikt zijn indien het beschreven systeem geen systeem is dat transacties verwerkt, indien het systeem bijvoorbeeld verband houdt met algemene interne beheersingsmaatregelen (general controls) met betrekking tot de hosting van een IT-applicatie, maar niet met de interne beheersingsmaatregelen die in de applicatie zelf zijn verankerd.

Materialiteit (Zie Par. 19 en 54)

A16. Bij een opdracht om verslag uit te brengen over de interne beheersingsmaatregelen bij een serviceorganisatie houdt het begrip materialiteit verband met het systeem waarover gerapporteerd wordt, niet met de financiële overzichten van gebruikersorganisaties. De IT-auditor van de serviceorganisatie plant werkzaamheden en voert deze uit om te bepalen of de beschrijving van de serviceorganisatie van haar systeem in alle van materieel belang zijnde opzichten getrouw is weergegeven, of de interne beheersingsmaatregelen bij de serviceorganisatie op afdoende wijze en in alle van materieel belang zijnde opzichten zijn opgezet en, in het geval van een type 2 rapport, of de interne beheersingsmaatregelen in alle van materieel belang zijnde opzichten effectief werken. Het begrip materialiteit houdt rekening met het feit dat het assurance-rapport van de IT-auditor van de serviceorganisatie informatie over het systeem van de serviceorganisatie verschaft om aan de algemene informatiebehoefte van een brede groep gebruikersorganisaties en hun accountants te voldoen die inzicht hebben in de manier waarop er gebruik is gemaakt van dat systeem.

A17. Materialiteit met betrekking tot de getrouwe weergave van de beschrijving van de serviceorganisatie van haar systeem, en met betrekking tot de opzet van interne beheersingsmaatregelen, houdt voornamelijk het in overweging nemen van kwalitatieve factoren in, bijvoorbeeld: of de beschrijving de significante aspecten van het verwerken van significante transacties omvat; of de beschrijving relevante informatie weglaat of verkeerd voorstelt; en het vermogen van interne beheersingsmaatregelen, zoals ze zijn opgezet, om een redelijke mate van zekerheid te verschaffen dat interne beheersingsdoelstellingen zouden worden bereikt. Materialiteit met betrekking tot het oordeel van de IT-auditor van de serviceorganisatie over de werking van interne beheersingsmaatregelen houdt het in overweging nemen van zowel kwantitatieve als kwalitatieve factoren in, bijvoorbeeld: de toelaatbare mate en waargenomen mate waarin wordt afgeweken (een kwantitatieve aangelegenheid) en de aard en oorzaak van een waargenomen deviatie (een kwalitatieve aangelegenheid).

A18. Het begrip materialiteit wordt niet toegepast bij het, in de beschrijving van de toetsingen van interne beheersingmaatregelen, openbaar maken van de resultaten van die toetsingen wanneer deviaties zijn geïdentificeerd. Dit is zo omdat, in de bijzondere omstandigheden van een specifieke gebruikersorganisatie of accountant van de gebruiker, de deviatie significantie kan hebben naast het feit dat zij, naar het oordeel van de IT-auditor van de serviceorganisatie, voorkomt dat een interne beheersingsmaatregel effectief werkt. De interne beheersingsmaatregel waarmee de deviatie verband houdt, kan bijvoorbeeld bijzonder significant zijn bij het voorkomen dat een bepaald soort fout die mogelijk in bepaalde omstandigheden in de omstandigheden van de financiële overzichten van een gebruikersorganisatie van materieel belang zou kunnen zijn.

Het verwerven van inzicht in het systeem van de serviceorganisatie (Zie Par. 20)

A19. Het verwerven van inzicht in het systeem van de serviceorganisatie, met inbegrip van interne beheersingsmaatregelen die bij de reikwijdte van de opdracht zijn opgenomen, ondersteunt de IT-auditor van de serviceorganisatie bij:

- Het aanduiden van de grenzen van dat systeem en hoe het met andere systemen is gekoppeld.
- Het vaststellen of de beschrijving van de serviceorganisatie het systeem dat is opgezet en geïmplementeerd, getrouw weergeeft.
- Het verwerven van inzicht in de interne beheersing over het opstellen van de vermelding van de serviceorganisatie
- Het bepalen welke interne beheersingsmaatregelen noodzakelijk zijn om de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, te bereiken.
- Het vaststellen of de interne beheersingsmaatregelen op afdoende wijze zijn opgezet.
- Het, in het geval van een type 2 rapport, vaststellen of interne beheersingsmaatregelen effectief werkten.

A20. De werkzaamheden van de IT-auditor van de serviceorganisatie om dit inzicht te verkrijgen kunnen omvatten:

- Het verzoeken om inlichtingen bij personen binnen de serviceorganisatie die, naar het oordeel van de IT-auditor van de serviceorganisatie, relevante informatie kunnen hebben.
- Het observeren van activiteiten en het inspecteren van documenten, rapportages, uitgeprinte en elektronische vastleggingen van de verwerking van transacties.
- Het inspecteren van een selectie van overeenkomsten tussen de serviceorganisatie en gebruikersorganisaties om hun gemeenschappelijke voorwaarden te identificeren.
- Het herhalen van de uitvoering van de interne beheersingsmaatregelen.

Het verkrijgen van assurance- informatie met betrekking tot de beschrijving (Zie Par. 21 en 22)

A21. Het in overweging nemen van de volgende vragen kan de IT-auditor van de serviceorganisatie ondersteunen bij het bepalen of die aspecten van de beschrijving die bij de reikwijdte van de opdracht zijn inbegrepen in alle van materieel belang zijnde opzichten getrouw zijn weergegeven:

- Behandelt de beschrijving de belangrijkste aspecten van de verleende dienst (binnen de reikwijdte van de opdracht) waarvan redelijkerwijs zou kunnen worden verwacht dat zij relevant zijn voor de algemene behoeftes van een brede groep accountants van de gebruiker bij het plannen van hun controles van de financiële overzichten van gebruikersorganisaties?
- Is de beschrijving op een gedetailleerd niveau opgesteld waarvan redelijkerwijs zou kunnen worden verwacht dat die aan een brede groep accountants van de gebruiker voldoende informatie verschaft om inzicht te verwerven in de interne beheersing overeenkomstig Standaard 315 van NBA[14]? De beschrijving hoeft niet op ieder aspect van de verwerking van de serviceorganisatie of de aan gebruikersorganisaties verleende diensten in te spelen en hoeft niet dermate gedetailleerd te zijn om het een lezer mogelijk te maken de veiligheid of overige interne beheersingsmaatregelen bij de serviceorganisatie in gevaar te brengen
- Is de beschrijving op een zodanige manier opgesteld dat die geen informatie weglaat of verkeerd voorstelt die de algemene

behoeftes van besluiten van een brede groep van accountants van de gebruikers kan beïnvloeden? Bevat de beschrijving bijvoorbeeld significante weglatingen of onnauwkeurigheden bij het verwerken waarvan de IT-auditor van de serviceorganisatie op de hoogte is?

- Waar sommige vermelde interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem van de reikwijdte van de opdracht zijn uitgesloten, onderkent de beschrijving daar duidelijk die uitgesloten doelstellingen?
- Zijn de interne beheersingsmaatregelen die in beschrijving worden geïdentificeerd geïmplementeerd?
- Zijn aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie , indien aanwezig, adequaat beschreven? In de meeste gevallen is de beschrijving van interne beheersingsdoelstellingen dermate verwoord dat het mogelijk is dat de interne beheersingsdoelstellingen worden bereikt middels de werking van interne beheersingsmaatregelen die alleen door de serviceorganisatie zijn geïmplementeerd. Echter, in sommige gevallen kunnen de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld niet door de serviceorganisatie alleen worden bereikt, omdat het bereiken daarvan bepaalde interne beheersingsmaatregelen vereist die door gebruikersorganisaties moeten worden geïmplementeerd. Dit kan het geval zijn waar de interne beheersingsdoelstellingen bijvoorbeeld door een regelgevende of toezichthoudende instantie zijn gespecificeerd. Wanneer de beschrijving inderdaad aanvullende interne beheersingsmaatregelen van de gebruikersorganisatie bevat, identificeert de beschrijving separaat die interne beheersingsmaatregelen samen met de specifieke interne beheersingsdoelstellingen die niet alleen door de serviceorganisatie bereikt kunnen worden
- Indien er van de opname methode (inclusive methode) gebruik is gemaakt, identificeert de beschrijving dan separaat interne beheersingsmaatregelen bij de serviceorganisatie en interne beheersingsmaatregelen bij de subserviceorganisatie? Indien er van de uitsluitingmethode (carve-out methode) gebruik is gemaakt, identificeert de beschrijving de functies die door de subserviceorganisatie zijn uitgevoerd? Wanneer er van de uitsluitingmethode (carve-out methode) gebruik is gemaakt, hoeft de beschrijving niet de gedetailleerde verwerking of interne beheersingsmaatregelen bij de subserviceorganisatie te beschrijven.

A22. De werkzaamheden van de IT-auditor van de serviceorganisatie om de getrouwe weergave van de beschrijving te evalueren, kunnen omvatten:

- Het in overweging nemen van de aard van gebruikersorganisaties en op welke wijze de diensten die door de serviceorganisatie zijn verleend deze waarschijnlijk beïnvloeden, bijvoorbeeld of gebruikersorganisaties afkomstig zijn uit een bepaalde sector en of zij door instanties binnen de overheid worden gereguleerd.
- Het lezen van standaardcontracten, of standaardvoorwaarden van contracten, (indien van toepassing) met gebruikersorganisaties om inzicht te krijgen in de contractuele verplichtingen van de serviceorganisatie.
- Het waarnemen van procedures die door het personeel van de serviceorganisatie zijn uitgevoerd.
- Het beoordelen van handleidingen met beleidslijnen en procedures en overige documentatie van de systemen zoals stroomschema's en beschrijvingen.

A23. Op grond van paragraaf 21(a) wordt er van de IT-auditor van de serviceorganisatie vereist dat hij evalueert of de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, redelijk zijn in de omstandigheden. Het in overweging nemen van de volgende vragen kan de IT-auditor van de serviceorganisatie ondersteunen bij deze evaluatie:

- Zijn de vermelde interne beheersingsdoelstellingen aangegeven door de serviceorganisatie of door externe partijen zoals een regelgevende of toezichthoudende instantie, een gebruikersgroep of een beroepsorganisatie die een transparant zorgvuldig proces volgt ?
- Waar de vermelde interne beheersingsdoelstellingen door de serviceorganisatie zijn gespecificeerd, houden zij daar verband met de soorten beweringen die doorgaans zijn vastgelegd in de financiële overzichten van een brede groep gebruikersorganisaties waarmee, naar redelijke verwachting, de interne beheersingsmaatregelen bij de serviceorganisatie verband houden? Alhoewel de IT-auditor van de serviceorganisatie doorgaans niet in staat is te bepalen op welke wijze interne beheersingsmaatregelen bij een serviceorganisatie specifiek verband houden met de beweringen die in de financiële overzichten van individuele gebruikersorganisaties zijn vastgelegd, wordt gebruik gemaakt van het inzicht van de IT-auditor van de serviceorganisatie in de aard van het systeem van de serviceorganisatie, met inbegrip van interne beheersingsmaatregelen, en in verleende diensten om de soorten beweringen te identificeren waarmee de interne beheersingsmaatregelen waarschijnlijk verband houden.
- Waar de vermelde interne beheersingsdoelstellingen door de serviceorganisatie zijn gespecificeerd, zijn zij daar volledig? Een complete set van interne beheersingsdoelstellingen kan aan een brede groep van accountants van de gebruiker een stelsel verschaffen om het effect van interne beheersingsmaatregelen bij de serviceorganisatie op de beweringen te beoordelen die doorgaans in de financiële overzichten van de gebruikersorganisaties zijn vastgelegd.

A24. De werkzaamheden van de IT-auditor van de serviceorganisatie om te bepalen of het systeem van de serviceorganisatie geïmplementeerd is, kan gelijk zijn aan, en uitgevoerd worden in samenhang met, werkzaamheden om een inzicht in dat systeem te verwerven. Zij kunnen ook het traceren van items door het systeem van de serviceorganisatie inhouden en, in het geval van een type 2 rapport, specifieke verzoeken om inlichtingen over de wijzigingen in interne beheersingsmaatregelen die gedurende die verslagperiode zijn geïmplementeerd. Wijzigingen die significant zijn voor gebruikersorganisaties of hun accountants zijn bij de beschrijving van de serviceorganisatie van haar systeem inbegrepen.

[14] NBA Standaard 315, "Risico's op een afwijking van materieel belang identificeren en het inschatten door inzicht te verwerven van in de entiteit en haar omgeving."

Het verkrijgen vanassurance- informatie met betrekking tot de opzet van interne beheersingsmaatregelen (Zie Par. 23 en 28(b))

A25. Vanuit het oogpunt van een *gebruikenrsorganisatie* of een *accountant van de gebruiker* is een interne beheersingsmaatregel op afdoende wijze opgezet indien zij, individueel of in combinatie met overige interne beheersingsmaatregelen, wanneer zij naar tevredenheid wordt nageleefd, een redelijke mate van zekerheid zou verschaffen dat afwijkingen van materieel belang worden voorkomen of zijn ontdekt of gecorrigeerd. Een *serviceorganisatie* of een *IT-auditor van de serviceorganisatie* is echter niet op de hoogte van de omstandigheden bij individuele gebruikersorganisaties die zouden bepalen of een afwijking van het materieel belang die het gevolg is van een deviatie van een interne beheersingsmaatregel voor die gebruikersorganisaties van materieel belang is. Derhalve is, vanuit het oogpunt van een IT-auditor van de serviceorganisatie, een interne beheersingsmaatregel op afdoende wijze opgezet, indien zij, individueel of in combinatie van overige interne beheersingsmaatregelen, wanneer zij naar tevredenheid wordt nageleefd, een redelijke mate van zekerheid zou verschaffen dat de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, worden bereikt.

A26. Een IT-auditor van de serviceorganisatie kan overwegen gebruik te maken van stroomschema's, vragenlijsten of beslissingstabellen om het inzicht in de opzet van interne beheersingsmaatregelen te bevorderen.

A27. Interne beheersingsmaatregelen kunnen uit een aantal activiteiten bestaan die bedoeld zijn om een interne beheersingsdoelstelling te bereiken. Derhalve is het mogelijk dat, indien de IT-auditor van de serviceorganisatie bepaalde activiteiten niet effectief acht voor het bereiken van een bepaalde interne beheersingsdoelstelling, het bestaan van overige activiteiten het voor de IT-auditorvan de serviceorganisatie mogelijk maakt dat hij concludeert dat de interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstelling op afdoende wijze zijn opgezet.

Het verkrijgen van assurance- informatie met betrekking tot de werking van interne beheersingsmaatregelen

Het vaststellen van de werking (Zie Par. 24)

A28. Vanuit het oogpunt van een gebruikersorganisatie of een accountant van de gebruiker werkt een interne beheersingsmaatregel effectief indien, individueel of in combinatie met overige interne beheersingsmaatregelen, zij een redelijke mate van zekerheid verschaft dat de afwijkingen van materieel belang, als gevolg van fraude of van fouten, worden voorkomen, of gedetecteerd en gecorrigeerd. Een serviceorganisatie of een IT-auditor van de serviceorganisatie, is echter niet op de hoogte van de omstandigheden bij individuele gebruikersorganisaties die zouden bepalen of een afwijking die het gevolg is van een deviatie van een interne beheersingsmaatregel is voorgekomen en, zo ja, of deze van materieel belang is. Daarom werkt, vanuit het oogpunt van de IT-auditor van de serviceorganisatie een interne beheersingsmaatregel effectief indien, individueel of in combinatie met overige interne beheersingsmaatregelen, zij een redelijke mate van zekerheid verschaft dat de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, worden bereikt. Op vergelijkbare wijze bevindt een serviceorganisatie of een IT-auditor van de serviceorganisatie zich niet in een positie om te bepalen of een waargenomen deviatie van een interne beheersingsmaatregel zou resulteren in een afwijking van materieel belang vanuit het oogpunt van een individuele gebruikersorganisatie.

A29. Het verkrijgen van inzicht in interne beheersingsmaatregelen dat voldoende is om een oordeel te vormen over de geschiktheid van hun opzet is niet voldoende assurance- informatie met betrekking tot hun werking, tenzij er een bepaald automatisme bestaat dat zorgt voor de consistente werking van de interne beheersingsmaatregelen zoals deze zijn opgezet en geïmplementeerd. Het verkrijgen van informatie over bijvoorbeeld het implementeren van een handmatige interne beheersingsmaatregel op een gegeven tijdstip verschaft geen assurance- informatie over de werking van interne beheersingsmaatregelen op andere tijdstippen. Vanwege de inherente consistentie van geautomatiseerde gegevensverwerking, kan het uitvoeren van werkzaamheden om de opzet van een geautomatiseerd interne beheersingsmaatregel te bepalen, en of deze geïmplementeerd is, mogelijk als assurance-informatie dienen die de werking van de interne beheersingsmaatregelen aantoont, afhankelijk van de beoordeling en toetsing van overige interne beheersingsmaatregelen zoals die over de wijzigingen in programma's.

A30. Om nuttig te zijn voor de accountant van de gebruiker, omvat een type 2 rapport doorgaans een minimale verslagperiode van zes maanden. Indien die verslagperiode korter is dan zes maanden, kan de IT-auditor van de serviceorganisatie het gepast achten om de redenen voor die kortere verslagperiode in het assurance-rapport van de IT-auditorvan de serviceorganisatie te beschrijven. Bij de omstandigheden die kunnen resulteren in een rapportage die een verslagperiode van minder dan zes maanden omvat, zijn onder meer inbegrepen wanneer (a) de IT-auditor van de serviceorganisatie tot dicht bij de datum waarop de rapportage over de interne beheersingsmaatregelen wordt uitgebracht een opdracht heeft; (b) de serviceorganisatie (of een bepaald systeem of toepassing) minder dan zes maanden heeft gewerkt; of (c) wanneer er significante wijzigingen in de interne beheersingsmaatregelen hebben plaatsgevonden en het niet praktisch uitvoerbaar is om zes maanden te wachten voordat de rapportage wordt uitgebracht of een rapportage uit te brengen die zowel de verslagperiodes voor als na de wijzigingen omvat.

A31. Bepaalde interne beheersingsmaatregelen kunnen geen assurance- informatie achterlaten over hun werking die op een latere datum kan worden getoetst en derhalve kan de IT-auditor van de serviceorganisatie het noodzakelijk achten om op verschillende tijdstippen gedurende de verslagperiode de werking van dergelijke interne beheersingsmaatregelen te toetsen.

A32. De IT-auditorvan de serviceorganisatie verschaft een oordeel over de werking van interne beheersingsmaatregelen gedurende iedere verslagperiode en daarom is er voldoende geschikte assurance- informatie over de werking van interne beheersingsmaatregelen gedurende de lopende verslagperiode vereist, zodat de IT-auditor van de serviceorganisatie dat oordeel kan verschaffen. Kennis van deviaties die in eerdere opdrachten zijn waargenomen kan er echter toe leiden dat de IT-auditor van de serviceorganisatie de omvang van het toetsen gedurende de lopende verslagperiode vergroot.

Het toetsen van indirecte beheersingsmaatregelen (Zie Par. 25(b))

A33. In sommige omstandigheden kan het noodzakelijk zijn om assurance- informatie te verkrijgen die de werking van indirecte beheersingsmaatregelen ondersteunt. Wanneer de IT-auditor van de serviceorganisatie bijvoorbeeld besluit om de effectiviteit van een beoordeling van uitzonderingsrapportages te toetsen die verkopen boven de toegestane kredietlimieten gedetailleerd beschrijven, is die beoordeling en de daarmee verband houdende follow-up de interne beheersingsmaatregel die voor de IT-auditor van de serviceorganisatie direct relevant is. Interne beheersingsmaatregelen betreffende de nauwkeurigheid van de informatie in de rapportages (bijvoorbeeld, de algemene interne beheersingsmaatregelen met betrekking tot IT (general IT controls) worden beschreven als "indirecte" interne beheersingsmaatregelen.

A34. Vanwege de inherente consistentie van geautomatiseerde gegevensverwerking, kan assurance- informatie over het implementeren van een geautomatiseerde interne beheersingsmaatregel op het niveau van de applicatie (application control), in combinatie met assurance- informatie over de werking van de algemene interne beheersingsmaatregelen van de serviceorganisatie (in het bijzonder, interne beheersingsmaatregelen betreffende wijzigingen) ook substantiële assurance-informatie over die werking verschaffen.

Manieren om items voor het toetsen te selecteren (Zie Par. 25(c) en 27)

A35. De manieren om elementen voor het toetsen te selecteren die beschikbaar zijn voor de IT-auditor van de serviceorganisatie:

(a) Het selecteren van alle elementen (100% onderzoek). Dit kan geschikt zijn bij het toetsen van interne beheersingsmaatregelen die niet frequent worden toegepast, ieder kwartaal bijvoorbeeld, of wanneer assurance- informatie met betrekking to het toepassen van de interne beheersingsmaatregel het onderzoek 100% effectief maakt;

(b) Het selecteren van specifieke elementen. Dit kan van toepassing zijn waar 100% onderzoek niet efficiënt zou zijn en een steekproef niet effectief zou zijn, zoals bij het toetsen van interne beheersingsmaatregelen die niet afdoende frequent zijn toegepast om een grote populatie voor een steekproef op te leveren, zoals interne beheersingsmaatregelen die maandelijks of wekelijks worden toegepast; en

(c) Het gebruiken van steekproeven. Dit kan van toepassing zijn bij het toetsen van interne beheersingsmaatregelen die frequent op een uniforme manier worden toegepast en die via documenten onderbouwde informatie van hun toepassing achterlaten.

A36. Terwijl selectief onderzoek van specifieke elementen vaak een effectieve manier zal zijn om assurance- informatie te verkrijgen, vertegenwoordigt het niet het gebruiken van steekproeven. De resultaten van werkzaamheden die worden toegepast op elementen die op deze manier zijn geselecteerd, kunnen niet op de gehele populatie worden geprojecteerd; dienovereenkomstig verschaft selectief onderzoek van specifieke elementen geen assurance- informatie met betrekking tot het restant van de populatie. Het gebruiken van steekproeven, aan de andere kant, is opgezet om het mogelijk te maken dat er conclusies worden getrokken over een gehele populatie op basis van het toetsen van een steekproef die daaruit genomen is.

De werkzaamheden van een interne auditfunctie

Het verwerven van inzicht in de interne auditfunctie (Zie Par. 30)

A37. Een interne auditfunctie kan verantwoordelijk zijn voor het verschaffen van analyses, evaluatie, zekerheid, aanbevelingen en overige informatie voor het management en de met governance belaste personen. Een interne auditfunctie bij een serviceorganisatie kan activiteiten uitvoeren die verband houden met het interne beheersingssysteem van de serviceorganisatie zelf of activiteiten die verband houden met de diensten en systemen, met inbegrip van interne beheersingsmaatregelen, die de serviceorganisatie aan gebruikersorganisaties verschaft.

Bepalen of en in welke mate er van de werkzaamheden van de interne auditors gebruik kan worden gemaakt (Zie Par. 33)

A38. Bij het bepalen van de geplande invloed van de werkzaamheden van de interne auditors op de aard, timing of omvang van de

werkzaamheden van de IT-auditor van de serviceorganisatie, kunnen de volgende factoren wijzen op de behoefte aan andere of minder uitgebreide werkzaamheden dan anders het geval zou zijn geweest:

- De aard en de reikwijdte van de door de interne auditors uitgevoerde, of nog uit te voeren, specifieke werkzaamheden, is nogal beperkt.
- De werkzaamheden van de interne auditors die verband houden met interne beheersingsmaatregelen die voor de conclusies van de IT-auditor van de serviceorganisatie minder significant zijn.
- Op grond van de werkzaamheden die door de interne auditors zijn uitgevoerd, of nog uitgevoerd moeten worden, worden geen subjectieve of complexe oordelen vereist.

Gebruikmaken van de werkzaamheden van de interne auditfunctie (Zie Par. 34)

A39. De aard, timing en omvang van de werkzaamheden van de IT-auditor van de serviceorganisatie betreffende specifieke werkzaamheden van de interne auditors zal afhankelijk zijn van de inschatting van de significantie van die werkzaamheden op de conclusies van de IT-auditor van de serviceorganisatie (bijvoorbeeld de significantie van de risico's waar de getoetste interne beheersingsmaatregelen ernaar streven deze te mitigeren), de evaluatie van de interne auditfunctie en de evaluatie van de specifieke werkzaamheden van de interne auditors. Dergelijke werkzaamheden kunnen omvatten:

- Het onderzoeken van elementen die reeds door de interne auditors zijn onderzocht;
- Het onderzoeken van andere soortgelijke elementen; en
- Het observeren van werkzaamheden die door de interne auditors zijn uitgevoerd.

Het effect op het assurance-rapport van de IT-auditor van de serviceorganisatie. (Zie Par. 36 en 37)

A40. Ongeacht de mate van autonomie en objectiviteit van de interne auditfunctie is een dergelijke functie niet onafhankelijk van de serviceorganisatie zoals van de IT-auditor van de serviceorganisatie bij het uitvoeren van de opdracht wel wordt verwacht. De IT-auditor van de serviceorganisatie heeft de ongedeelde verantwoordelijkheid voor het oordeel dat in het assurance-rapport van de IT-auditor van de serviceorganisatie tot uitdrukking wordt gebracht en die verantwoordelijkheid wordt niet verminderd doordat de IT-auditor van de serviceorganisatie gebruik maakt van de werkzaamheden van de interne IT-auditors.

A41. De beschrijving van de IT-auditor van de serviceorganisatie van de werkzaamheden die door de interne auditfunctie worden uitgevoerd kan op meerdere manier worden weergegeven, zoals:

- Door introductiemateriaal op te nemen in de beschrijving van de toetsing van interne beheersingsmaatregelen die erop wijst dat er van bepaalde werkzaamheden van de interne auditfunctie gebruik werd gemaakt bij het uitvoeren van toetsingen van interne beheersingsmaatregelen.
- De toeschrijving van individuele toetsingen aan de interne auditafdeling.

Schriftelijke bevestigingen (Zie Par. 38 en 40)

A42. De schriftelijke bevestigingen die op grond van paragraaf 38 worden vereist staan los van, en zijn een aanvulling op, de vermelding van de serviceorganisatie zoals die in paragraaf 9(o) staat beschreven.

A43. Indien de serviceorganisatie de schriftelijke bevestigingen die overeenkomstig paragraaf 38 (c) van deze Richtlijn worden vereist niet verschaft, kan het voor het oordeel van de IT-auditor van de serviceorganisatie van toepassing zijn om overeenkomstig paragraaf 55(d) van deze Richtlijn te worden aangepast.

Overige Informatie (Zie Par. 42)

A44. Op grond van het Reglement Gedragscode ('Code of Ethics') wordt er van de IT-auditor van de serviceorganisatie vereist dat hij niet met informatie mag worden geassocieerd waarvan de IT-auditor van de serviceorganisatie aanneemt dat de informatie:

(a) Een materieel onjuiste of misleidende vermelding bevat;
(b) Onzorgvuldig verschafte vermeldingen of informatie bevat; of
(c) Informatie weglaat of verbergt waarvan is vereist dat die informatie is toegevoegd waar een dergelijke weglating of verberging misleidend zou kunnen zijn[15].

Indien overige informatie die bij een document is ingesloten dat de beschrijving van de serviceorganisatie van haar systeem bevat en het assurance-rapport van de IT-auditor van de serviceorganisatie toekomstgerichte informatie bevat zoals herstel en uitwijk, rampen (bestrijdings) -plannen of plannen voor aanpassingen aan het systeem die zullen inspelen op deviaties die in het assurance-rapport van de IT-auditorvan de serviceorganisatie zijn geïdentificeerd of claims van een promotionele aard die niet op een aanvaardbare manier kunnen worden gestaafd, kan de IT-auditor van de serviceorganisatie erom verzoeken dat die informatie wordt verwijderd of wordt aangepast.

A45. Indien de serviceorganisatie weigert om de overige informatie te verwijderen of aan te passen, kunnen aanvullende activiteiten die van toepassing zijn het volgende omvatten:

- De serviceorganisatie verzoeken om met haar juridische adviseurs overleg te plegen met betrekking tot de handelswijzen.
- Het beschrijven van de van materieel belang zijnde inconsistentie of afwijking van materieel belang van feiten in het assurance-rapport.
- Het niet verstrekken van het assurance-rapport totdat de aangelegenheid is opgelost.
- De opdracht teruggeven.

Documentatie (Zie Par.. 51)

A46. In de wet- en regelgeving op het gebied van kwaliteitsbeheersing wordt er vereist dat er beleidslijnen en procedures worden vastgesteld voor het tijdig afronden van het samenstellen van opdrachtdossiers[16]. Een geschikte tijdslimiet waarbinnen de samenstelling van het definitieve opdrachtdossier moet worden afgerondis gewoonlijk niet meer dan 60 dagen na de datum van het assurance-rapport[17].

Het opstellen van het assurance-rapport van de IT-auditor **van de serviceorganisatie**

Inhoud van het assurance-rapport van de IT-auditor van de serviceorganisatie (Zie Par. 53)

A47. Voorbeelden ter illustratie van assurance-rapporten van IT-auditor van de serviceorganisatie en daarmee verband houdende vermeldingen van serviceorganisaties staan in bijlagen 1en 2.

Beoogde gebruikers en doeleinden van het assurance-rapport van de IT-auditor van de serviceorganisatie (Zie Par. 53(e))

A48. De criteria waarvan gebruik wordt gemaakt voor opdrachten om te rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie zijn alleen relevant voor de doeleinden van het verschaffen van informatie over het systeem van de serviceorganisatie, met inbegrip van interne beheersingsmaatregelen, aan degenen die inzicht hebben op welke wijze er van het systeem gebruik is gemaakt bij de financiële verslaggeving door gebruikersorganisaties. Dienovereenkomstig staat dit in het assurance-rapport van de IT-auditorvan de serviceorganisatie vermeld. De IT-auditor van de serviceorganisatie kan het passend achten om bewoordingen op te nemen die de specifieke verspreiding van het assurance-rapport onder anderen dan de beoogde gebruikers, of het gebruik ervan voor andere doeleinden, beperkt.

Beschrijving van de toetsingen van interne beheersingsmaatregelen (Zie Par. 54)

A49. Bij het beschrijven van de aard van de toetsingen van interne beheersingsmaatregelen voor een type 2 rapport, worden de lezers van het assurance-rapport van de IT-auditor van de serviceorganisatie ondersteund als de IT-auditor van de serviceorganisatie het volgende opneemt:

- De resultaten van alle toetsingen waar deviaties zijn geïdentificeerd, zelfs als er overige interne beheersingsmaatregelen zijn geïdentificeerd die de IT-auditor van de serviceorganisatie in staat stellen te concluderen dat de relevante interne beheersingsdoelstelling is bereikt of de getoetste interne beheersingsmaatregel nadien van de beschrijving van de

serviceorganisatie van haar systeem is verwijderd.

- Informatie over de veroorzakende factoren van geïdentificeerde deviaties, tot de mate waarin de IT-auditor van de serviceorganisatie die factoren heeft geïdentificeerd.

Aangepaste oordelen (Zie Par. 55)

A50. Voorbeelden ter illustratie van elementen van aangepaste assurance-rapporten van de IT-auditor van de serviceorganisatie staan in bijlage 3.

A51. Zelfs als de IT-auditor van de serviceorganisatie een afkeurend oordeel tot uitdrukking heeft gebracht of een oordeelonthouding heeft geformuleerd, kan het gepast zijn in de paragraaf voor de onderbouwing van het aangepaste oordeel de redenen voor overige aangelegenheden te beschrijven waarvan de IT-auditor van de serviceorganisatie weet dat op grond daarvan een aanpassing van het oordeel zou zijn vereist, alsmede de effecten daarvan.

[15] Reglement Gedragscode, Artikel A-110.2.
[16] Richtlijn Documentatie (NOREA 230) paragraaf 14.
[17] Richtlijn Documentatie (NOREA 230) paragraaf A21.

A52. Wanneer een oordeelonthouding wordt geformuleerd vanwege een beperking in de reikwijdte, is het doorgaans niet passend om de uitgevoerde werkzaamheden te vermelden noch om vermeldingen die de kenmerken van de opdracht van een IT-auditor van de serviceorganisatie beschrijven op te nemen; door dit wel te doen zou de oordeelonthouding kunnen worden overschaduwd.

Overige communicatieverantwoordelijkheden (Zie Par. 56)

A53. Geschikte activiteiten om in te spelen op de omstandigheden die paragraaf 56 zijn geïdentificeerd kunnen omvatten:

- Het verkrijgen van juridisch advies over de consequenties van verschillende handelswijzen.
- Communicatie met de met governance belaste personen van de serviceorganisatie.
- Communicatie met derden (bijvoorbeeld, een regelgever of toezichthouder) wanneer dit vereist is.
- Het aanpassen van het oordeel van de IT-auditor van de serviceorganisatie of het toevoegen van een paragraaf inzake overige aangelegenheden.
- Het teruggeven vande opdracht.

BIJLAGE 1

(Zie Par. A47)

VOORBEELD VAN DE VERMELDINGEN VAN DE SERVICEORGANISATIE

De volgende voorbeelden van de vermeldingen van een serviceorganisatie zijn bestemd als leidraden en dienen niet op uitputtende wijze te worden gebruikt en zijn niet op alle situaties van toepassing.

Voorbeeld 1: Type 2 vermelding van een serviceorganisatie

Vermelding door een serviceorganisatie

De bijgaande beschrijving is voor cliënten opgesteld die gebruik hebben gemaakt van het [het soort of de naam van] systeem en voor hun accountants die voldoende inzicht hebben om de beschrijving, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door de cliënten zelf worden uitgevoerd, te beschouwen wanneer zij de risico's van afwijkingen van materieel belang van de financiële overzichten van de cliënten inschatten. [Naam van de entiteit] bevestigt dat:

(a) De bijgaande beschrijving op de pagina's [bb-cc] het [het soort of de naam van] systeem voor het verwerken van de transacties van de cliënten gedurende de verslagperiode van [datum] tot [datum] getrouw weergeeft. De criteria waarvan gebruik wordt gemaakt bij het maken van deze vermelding hielden in dat de bijgaande beschrijving:

(i) Weergeeft op welke wijze het systeem is opgezet en geïmplementeerd, met inbegrip van:
De soorten diensten die verleend zijn, met inbegrip van, in voorkomend geval de verwerkte transactiestromen.
De procedures, binnen zowel informatietechnologie als handmatige systemen, waardoor die transacties werden geïnitieerd, vastgelegd, verwerkt, gecorrigeerd voor zover noodzakelijk en overgebracht naar de rapportages die voor de cliënten zijn opgesteld.
De verbonden administratie, de ondersteunende informatie en specifieke rekeningen waarvan gebruik is gemaakt om transacties te initiëren, te verwerken en vast te leggen; dit houdt onder meer het corrigeren van incorrecte informatie in en op welke wijze informatie is overgedragen naar de rapportages die voor de cliënten zijn opgesteld.
Op welke wijze het systeem de significante gebeurtenissen en omstandigheden, buiten de transacties, heeft behandeld.
Het proces waarvan gebruik werd gemaakt bij het opstellen van rapportages voor cliënten.
Relevante interne beheersingsdoelstellingen en interne beheersingsmaatregelen die zijn opgezet om die doelstellingen te bereiken.
Interne beheersingsmaatregelen waarvan wij, bij de opzet van het systeem, aannamen dat zij door gebruikersorganisaties zouden worden geïmplementeerd en die, indien noodzakelijk om de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld te bereiken, samen met de specifieke interne beheersingsdoelstellingen die niet alleen door onszelf kunnen worden bereikt, zijn geïdentificeerd.
Overige aspecten van onze beheersingsomgeving, het risico-inschattingsproces, het informatiesysteem (met inbegrip van het verbonden bedrijfsproces) en communicatie, beheersingsactiviteiten en interne beheersingsmaatregelen in het kader van het monitoren die relevant zijn voor het verwerken en het rapporteren van de transacties van de cliënten.

(ii) Relevante details bevat van wijzigingen in het systeem van de serviceorganisatie gedurende de verslagperiode van [datum] tot [datum].

(iii) Geen informatie weglaat of verkeerd voorstelt die relevant is voor de reikwijdte van het systeem dat is beschreven terwijl erkend wordt dat de beschrijving is opgesteld om te voldoen aan de algemene behoeftes van een brede groep gebruikers en hun accountants en daarom niet ieder aspect van het systeem kan bevatten dat iedere individuele cliënt in diens eigen bijzonder omgeving belangrijk kan achten.

(b) De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld op afdoende wijze zijn opgezet en gedurende de verslagperiode van [datum] tot [datum] effectief werkten. De criteria waarvan bij het maken van deze vermelding gebruik werd gemaakt hielden in dat :

(i) De risico's die het bereiken van de interne beheersingsdoelstellingen die in de beschrijving staan vermeld in gevaar brengen, werden geïdentificeerd;

(ii) De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen; en

(iii) De interne beheersingsmaatregelen gedurende de verslagperiode van [datum] tot [datum] consistent zijn toegepast zoals opgezet, met inbegrip ervan dat handmatige interne beheersingsmaatregelen zijn toegepast door personen die de geschikte competentie en bevoegdheid hebben.

Voorbeeld 2: Type 1 Vermelding van een serviceorganisatie

De bijgaande beschrijving is opgesteld voor cliënten die gebruik hebben gemaakt van het [het soort of de naam van] systeem en voor hun accountants die voldoende inzicht hebben om de beschrijving te beschouwen, samen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door de cliënten zelf worden beheerd, wanneer zij inzicht verwerven in de informatiesystemen van cliënten die relevant zijn voor financiële verslaggeving. [Naam van de entiteit] bevestigt dat:

(a) De bijgaande beschrijving op de pagina's [bb-cc] geeft het [het soort of de naam van] systeem voor het verwerken van de transacties van de cliënten gedurende de verslagperiode op [datum] getrouw weer. De criteria waarvan gebruik wordt gemaakt bij het maken van deze vermelding hielden in dat de bijgaande beschrijving:

(i) Weergeeft op welke wijze het systeem is opgezet en geïmplementeerd, met inbegrip van:

De soorten diensten die verleend zijn, met inbegrip van, in voorkomend geval, de verwerkte transactiestromen.

De procedures, binnen zowel informatietechnologie als handmatige systemen, waardoor die transacties werden geïnitieerd, vastgelegd, verwerkt, gecorrigeerd voor zover noodzakelijk en overgebracht naar de rapportages die voor de cliënten zijn opgesteld.

De verbonden administratie, die de informatie en specifieke rekeningen waarvan gebruik is gemaakt om transacties te initiëren, verwerken, vast te leggen en rapporteren; dit houdt onder meer het corrigeren van incorrecte informatie in en op welke wijze informatie is overgedragen naar de rapportages die voor de cliënten zijn opgesteld.

Op welke wijze het systeem de significante gebeurtenissen en omstandigheden, buiten de transacties, heeft behandeld.

Het proces waarvan gebruik werd gemaakt bij het opstellen van rapportages voor cliënten.

Relevante interne beheersingsdoelstellingen en interne beheersingsmaatregelen die zijn opgezet om die doelstellingen te bereiken.

Interne beheersingsmaatregelen waarvan wij, bij de opzet van het systeem, aannamen dat zij door gebruikersorganisaties zouden worden geïmplementeerd en die, indien noodzakelijk om de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld te bereiken, samen met de specifieke interne beheersingsdoelstellingen die niet alleen door onszelf kunnen worden bereikt zijn geïdentificeerd.

Overige aspecten van onze beheersingsomgeving, het risico-inschattingsproces, het informatiesysteem (met inbegrip van het verbonden bedrijfsproces) en communicatie, beheersingsactiviteiten en interne beheersingsmaatregelen betreffende monitoring die relevant zijn voor het verwerken en het rapporteren van de transacties van de cliënten.

(ii) Geen informatie weglaat of verkeerd voorstelt die relevant is voor de reikwijdte van het systeem dat is beschreven terwijl erkend wordt dat de beschrijving is opgesteld om te voldoen aan de algemene behoeftes van een brede groep gebruikers en hun accountants en daarom niet ieder aspect van het systeem kan bevatten dat iedere individuele cliënt in diens eigen bijzondere omgeving belangrijk kan achten.

(b) De interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de bijgaande beschrijving staan vermeld op afdoende wijze zijn opgezet, op [datum]. De criteria waarvan bij het maken van deze vermelding gebruik werd gemaakt hielden in dat:

(i) De risico's die het bereiken van de interne beheersingsdoelstellingen die in de beschrijving staan vermeld in gevaar brengen, werden geïdentificeerd; en

(ii) De onderkende interne beheersingsmaatregelen, indien zij werkzaam zijn zoals beschreven, een redelijke mate van zekerheid zouden verschaffen dat die risico's het bereiken van de vermelde interne beheersingsdoelstellingen niet zouden verhinderen.

BIJLAGE 2

(Zie Par. A47)

Voorbeelden van de assurance-rapporten van de IT-auditor van de serviceorganisatie

De volgende voorbeelden van rapporten zijn bestemd als leidraden en dienen niet op uitputtende wijze te worden gebruikt en zijn niet op alle situaties van toepassing.

Voorbeeld 1: Type 2 assurance-rapport van de IT-auditor van de serviceorganisatie.

Assurance-rapport van de onafhankelijke IT-auditor van de serviceorganisatie over de beschrijving van interne beheersingsmaatregelen, hun opzet en werking.

Aan: XYZ Serviceorganisatie

Reikwijdte

Wij hebben opdracht gekregen om te rapporten over de beschrijving van XYZ serviceorganisatie op de pagina's [bb-cc] van haar [het soort of de naam van] systeem voor het verwerken van de transacties van cliënten gedurende de verslagperiode van [datum] tot [datum] (de beschrijving), en over de opzet en werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld[18].

Verantwoordelijkheden van XYZ serviceorganisatie

XYZ serviceorganisatie is verantwoordelijk voor: het opstellen van de beschrijving en bijgaande vermelding op pagina [aa], met inbegrip van de volledigheid, nauwkeurigheid en methode van presentatie van de beschrijving en vermelding; het verlenen van diensten die door de beschrijving worden omvat; het vermelden van de interne beheersingsdoelstellingen; het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om de vermelde interne beheersingsdoelstellingen te bereiken.

[18] Indien sommige elementen van de beschrijving niet bij de reikwijdte van de opdracht zijn inbegrepen, wordt dit in het assurance-rapport duidelijk gemaakt.

Onze onafhankelijkheid en kwaliteitsbeheersing

Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag.

De IT-auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving

Verantwoordelijkheden van de IT-auditor van de serviceorganisatie

Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van een oordeel over de beschrijving van XYZ serviceorganisatie en over de opzet en werking van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld. We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder Richtlijn 3402 "Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie" vastgesteld door Nederlandse Orde van Register EDP-Auditors (NOREA). Dit vereist dat wij onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of, in alle van materieel belang zijnde aspecten, de beschrijving getrouw is weergegeven en de interne beheersingsmaatregelen op afdoende wijze zijn opgezet en effectief werken.

Een assurance-opdracht om te rapporteren over de beschrijving, opzet en werking van interne beheersingsmaatregelen bij een serviceorganisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de toelichtingen in de beschrijving van de serviceorganisatie van haar systeem en de opzet en werking van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de IT-auditor van de serviceorganisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de beschrijving niet getrouw is weergegeven en dat interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet of effectief werken. Onze werkzaamheden bevatten het toetsen van de werking van die interne beheersingsmaatregelen die wij noodzakelijk achten bij het verschaffen van een redelijke mate van zekerheid dat de interne beheersingsdoelstellingen die in de beschrijving staan vermeld werden bereikt. Een assurance-opdracht van dit type omvat ook een evaluatie van het algehele beeld van de beschrijving, de geschiktheid van de interne beheersingsdoelstellingen die erin staan vermeld en de geschiktheid van de criteria die door de serviceorganisatie zijn gespecificeerd en beschreven staan op pagina [aa].

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel te bieden.

Beperkingen van interne beheersingsmaatregelen bij een serviceorganisatie

De beschrijving van XYZ serviceorganisatie is opgezet om aan de algemene behoeftes van een brede groep van cliënten en hun accountants te voldoen en kan daarom niet ieder aspect van het systeem bevatten dat iedere individuele cliënt in diens eigen bijzondere omgeving belangrijk kan achten. Bovendien kunnen interne beheersingsmaatregelen bij een serviceorganisatie, vanwege hun aard, niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken. Bovendien is de projectie van een eventuele evaluatie van de effectiviteit naar toekomstige verslagperiodes onderhevig aan het risico dat interne beheersingsmaatregelen bij een serviceorganisatie inadequaat kunnen worden of falen.

Oordeel

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van XYZ serviceorganisatie op pagina [aa] staan beschreven. Naar ons oordeel, in alle van materieel belang zijnde aspecten:

(a) Geeft de beschrijving het [het soort of de naam] systeem getrouw weer zoals deze gedurende de verslagperiode van [datum] tot [datum]is opgezet en geïmplementeerd;

(b) Zijn de interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld gedurende de verslagperiode van [datum] tot [datum]op afdoende wijze opgezet; en

(c) Werkten de getoetste interne beheersingsmaatregelen, die noodzakelijk waren om een redelijke mate van zekerheid te verschaffen dat de in de beschrijving vermelde interne beheersingsdoelstellingen waren bereikt, gedurende de verslagperiode van [datum] tot [datum] effectief.

Beschrijving van getoetste interne beheersingsmaatregelen

De specifieke getoetste interne beheersingsmaatregelen en de aard, timing en resultaten van die toetsingen zijn opgenomen op pagina's [yy-zz].

Beoogde gebruikers en doel

Deze rapportage en de beschrijving van toetsingen van interne beheersingsmaatregelen op pagina's [yy-zz] zijn alleen voor cliënten die gebruik hebben gemaakt van het [het soort of naam van] systeem van de XYZ serviceorganisatie en hun accountants, die voldoende inzicht hebben om het in aanmerking te nemen bij het inschatten van de risico's op afwijkingen van het materieel belang in de financiële overzichten van de cliënten tezamen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door cliënten zelf worden uitgevoerd.

[Handtekening van IT-auditor van de serviceorganisatie]

[Datum van het assurance-rapport van deIT-auditor van de serviceorganisatie]

[Het adres van deIT-auditor van de serviceorganisatie]

Voorbeeld 2: Type 1 assurance-rapport van deIT-auditor van de serviceorganisatie

Assurance-rapport van de onafhankelijkeIT-auditor van de serviceorganisatie over de beschrijving van interne beheersingsmaatregelen en hun opzet

Aan XYZ Serviceorganisatie

Reikwijdte

Wij hebben opdracht gekregen om te rapporteren over de beschrijving van XYZ serviceorganisatie op de pagina's [bb-cc] van haar [het soort of de naam van] systeem voor het verwerken van de transacties van cliënten op [datum] (de beschrijving), en over de opzet van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld[19].
Wij hebben geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen die bij de beschrijving zijn inbegrepen en brengen daarover geen oordeel tot uitdrukking.
Verantwoordelijkheden van XYZ Serviceorganisatie
XYZ serviceorganisatie is verantwoordelijk voor: het opstellen van de beschrijving en bijgaande vermelding op pagina [aa], met inbegrip van de volledigheid, nauwkeurigheid en methode van presentatie van de beschrijving en de bewering; het verlenen van diensten die door de beschrijving worden omvat; het vermelden van de interne beheersingsdoelstellingen; het opzetten, implementeren en effectief laten werken van interne beheersingsmaatregelen om de vermelde interne beheersingsdoelstellingen te bereiken.
Onze onafhankelijkheid en kwaliteitsbeheersing
Wij hebben de vereisten van het Reglement Gedragscode ('Code of Ethics') van NOREA nageleefd, welke is gebaseerd is op de fundamentele beginselen van integriteit, objectiviteit, deskundigheid en zorgvuldigheid, geheimhouding en professioneel gedrag. De IT-auditeenheid past het Reglement Kwaliteitsbeheersing NOREA (RKBN) toe en bijgevolg onderhoudt het een uitgebreid systeem van kwaliteitscontrole met inbegrip van gedocumenteerd beleid en de procedures met betrekking tot de naleving van de ethische voorschriften, professionele standaarden en de van toepassing zijnde wet- en regelgeving
Verantwoordelijkheden van de IT-auditor van de serviceorganisatie
Onze verantwoordelijkheid is, op basis van onze werkzaamheden, het geven van een oordeel over de beschrijving van XYZ serviceorganisatie en over de opzet van interne beheersingsmaatregelen die verband houden met de interne beheersingsdoelstellingen die in de beschrijving staan vermeld. We hebben onze opdracht uitgevoerd overeenkomstig Nederlands recht, waaronder Richtlijn 3402 "Assurance-rapporten betreffende interne beheersingsmaatregelen bij een serviceorganisatie" vastgesteld door Nederlandse Orde van Register EDP-Auditors (NOREA). Dit vereist dat wij onze werkzaamheden zodanig plannen en uitvoeren dat een redelijke mate van zekerheid wordt verkregen over de vraag of de beschrijving getrouw is weergegeven en de interne beheersingsmaatregelen, in alle van materieel belang zijnde aspecten, op afdoende wijze zijn opgezet.
Een assurance-opdracht om te rapporteren over de beschrijving en opzet van interne beheersingsmaatregelen bij een serviceorganisatie omvat het uitvoeren van werkzaamheden ter verkrijging van assurance-informatie over de toelichtingen in de beschrijving van de serviceorganisatie van haar systeem en de opzet van interne beheersingsmaatregelen. De geselecteerde werkzaamheden zijn afhankelijk van de door de IT-auditor van de serviceorganisatie toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de beschrijving niet getrouw is weergegeven en dat interne beheersingsmaatregelen niet op afdoende wijze zijn opgezet. Een assurance-opdracht van dit type omvat ook het evalueren van het algehele beeld van de beschrijving, de geschiktheid van de interne beheersingsdoelstellingen die daarin staan vermeld en de geschiktheid van de criteria die door de serviceorganisatie zijn gespecificeerd en die staan beschreven op pagina [aa].
Zoals hierboven staat vermeld, hebben wij geen werkzaamheden uitgevoerd met betrekking tot de werking van interne beheersingsmaatregelen die bij de beschrijving waren inbegrepen en brengen derhalve daarover geen oordeel tot uitdrukking.
Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel te bieden.
Beperkingen van interne beheersingsmaatregelen bij een serviceorganisatie
De beschrijving van XYZ serviceorganisatie is opgezet om aan de algemene behoeftes van een brede groep van cliënten en hun accountants te voldoen en kandaarom niet ieder aspect van het systeem bevatten dat iedere individuele cliënt in diens eigen bijzondere omgeving belangrijk kan achten. Bovendien kunnen interne beheersingsmaatregelen bij een serviceorganisatie, vanwege hun aard, niet alle fouten of omissies bij het verwerken of rapporteren van transacties voorkomen of ontdekken.
Oordeel
Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van XYZ serviceorganisatie op pagina [aa]staan beschreven. Naar ons oordeel, in alle van materieel belang zijnde aspecten: (a) Geeft de beschrijving het [het soort of de naam van] systeem getrouw weer zoals deze op [datum] is opgezet en geïmplementeerd; (b) Zijn de interne beheersingsmaatregelen die verband houden met de in de beschrijving vermelde interne beheersingsdoelstellingen op [datum] op afdoende wijze opgezet.
Beoogde gebruikers en doel
Deze rapportage is alleen voor cliënten die gebruik hebben gemaakt van het [het soort of naam van] systeem van de XYZ serviceorganisatie en hun accountants, die voldoende inzicht hebben om het in aanmerking te nemen bij het verwerven van inzicht in de informatiesystemen van cliënten die relevant zijn voor financiële verslaggeving tezamen met overige informatie met inbegrip van informatie over interne beheersingsmaatregelen die door cliënten zelf worden uitgevoerd.
[Handtekening van de IT-auditor van de serviceorganisatie]
[Datum van het assurance-rapport van de IT-auditor van de serviceorganisatie]
[Het adres van de IT-auditorvan de serviceorganisatie]

Bijlage 3

(Zie Par. A50)

[19] Indien sommige elementen van de beschrijving niet bij de reikwijdte van de opdracht zijn inbegrepen, wordt dit in het assurance-rapport duidelijk gemaakt.

Voorbeeld aangepast assurance-rapport van de IT-auditor van de serviceorganisatie

De volgende voorbeelden van aangepaste rapporten zijn bestemd als leidraden en zijn niet uitputtend of van toepassing op alle situaties. Zij zijn gebaseerd op de voorbeelden van rapportages in Bijlage 2.

Voorbeeld 1: Oordeel met beperking – de beschrijving van het systeem van de serviceorganisatie is niet getrouw weergegeven in alle van materieel belang zijnde aspecten

…

Verantwoordelijkheden van de IT-auditor van de serviceorganisatie

…

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om daarop een onderbouwing voor ons oordeel met beperking te bieden.

Onderbouwing van het oordeel met beperking

De bijgaande beschrijving vermeldt op pagina [mn] dat XYZ serviceorganisatie gebruik maakt van operator identificatienummers en wachtwoorden om onbevoegde toegang tot het systeem te voorkomen. Op basis van onze werkzaamheden, die onder meer verzoeken om inlichtingen van het stafpersoneel en waarneming van activiteiten inhouden, hebben wij bepaald dat operator identificatienummers en wachtwoorden in Applicatie A en B, maar niet in Applicatie C en D worden gebruikt.

Oordeel met beperking

Ons oordeel is gevormd op de basis van de aangelegenheden die in deze rapportage uiteen zijn gezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van XYZ serviceorganisatie op pagina [aa] staan beschreven. Naar ons oordeel, in alle van materieel belang zijnde opzichten uitgezonderd de aangelegenheid die staat beschreven in de paragraaf 'Onderbouwing van het oordeel met beperking'

(a) …

Voorbeeld 2: Oordeel met beperking – de interne beheersingsmaatregelen zijn niet op afdoende wijze opgezet om een redelijke mate van zekerheid te verschaffen dat de interne beheersingsdoelstellingen die in de beschrijving van de serviceorganisatie van haar systeem staan vermeld, bereikt zullen worden indien de interne beheersingsmaatregelen effectief werken.

…

Verantwoordelijkheden van de IT-auditor van de serviceorganisatie

…

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel met beperking te bieden.

Basis voor een oordeel met beperking

Zoals op pagina [mn] van de bijgaande beschrijving wordt besproken, brengt de XYZ serviceorganisatie zo nu en dan wijzigingen aan in applicatieprogramma's om tekortkomingen te corrigeren of om capaciteiten te verbeteren. De procedures die worden gevolgd bij het bepalen of er wijzigingen moeten worden aangebracht, bij het opzetten van de wijzigingen en het implementeren ervan, houden geen beoordeling en goedkeuring in door bevoegde personen die onafhankelijk zijn van de personen die betrokken zijn bij het aanbrengen van die wijzigingen. Er bestaan ook geen gespecificeerde vereisten om dergelijke wijzigingen te toetsen of om de toetsingsresultaten aan een bevoegde beoordelaar te verschaffen voordat de wijzigingen worden geïmplementeerd.

Oordeel met beperking

Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van de XYZ serviceorganisatie op pagina [aa] staan beschreven. Naar ons oordeel, in alle van materieel belang zijnde aspecten, uitgezonderd de aangelegenheid die staat beschreven in de paragraaf 'Onderbouwing van het oordeel met beperking':

(a) …

Voorbeeld 3: Oordeel met beperking – de interne beheersingsmaatregelen werkten gedurende de gespecificeerde verslagperiode niet effectief (alleen type 2 rapport)

…

Verantwoordelijkheden van de IT-auditor van de serviceorganisatie

…

Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel met beperking te bieden.

Onderbouwing voor oordeel met beperking
XYZ serviceorganisatie vermeldt in haar beschrijving dat zij geautomatiseerde interne beheersingsmaatregelen heeft om ontvangen uitbetalingen van loon te reconciliëren met de gegenereerde output. Zoals echter genoemd op pagina [mn] van de beschrijving, werkte deze interne beheersingsmaatregel gedurende de verslagperiode van dd/mm/jjjj tot dd/mm/jjjj niet effectief als gevolg van een programmeerfout. Dit resulteerde in het niet-bereiken van de interne beheersingsdoelstelling "Interne beheersingsmaatregelen verschaffen een redelijke mate van zekerheid dat de ontvangen uitbetalingen van loon behoorlijk worden vastgelegd" gedurende de verslagperiode van dd/mm/jjjj tot dd/mm/jjjj XYZ heeft een wijziging in het programma geïmplementeerd ten aanzien van de reconciliatie van loonuitbetalingen per [datum] en onze toetsingen wijzen erop dat het gedurende de verslagperiode van dd/mm/jjjj tot dd/mm/jjjj effectief werkte.
Oordeel met beperking
Ons oordeel is gevormd op basis van de aangelegenheden die in deze rapportage zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van de XYZ serviceorganisatie op pagina [aa] staan beschreven. In ons oordeel, in alle van materieel belang zijnde aspecten, uitgezonderd de aangelegenheid die staat beschreven in de paragraaf 'Onderbouwing van het oordeel met beperking':
…
Voorbeeld 4: Oordeel met beperking – de IT-auditor van de serviceorganisatie is niet in staat tot het verkrijgen van voldoende en geschikte assurance- informatie
…
Verantwoordelijkheden van de IT-auditor van de serviceorganisatie
…
Wij zijn van mening dat de door ons verkregen assurance-informatie voldoende en geschikt is om een onderbouwing voor ons oordeel met beperking te bieden.
Basis voor oordeel met beperking
XYZ serviceorganisatie vermeldt in haar beschrijving dat zij geautomatiseerde interne beheersingsmaatregelen heeft om ontvangen uitbetalingen van loon te reconciliëren met de gegenereerde output. De elektronische vastleggingen van de uitvoering van deze aansluiting voor de verslagperiode van dd/mm/jjjj tot dd/mm/jjjj zijn als resultaat van een computerverwerkingsfout verwijderd en om die reden waren wij niet in staat de werking van deze interne beheersingsmaatregel voor die verslagperiode te toetsen. Bijgevolg waren wij niet in staat te bepalen of de interne beheersingsdoelstelling "Interne beheersingsmaatregelen verschaffen een redelijke mate van zekerheid dat de ontvangen uitbetalingen van loon behoorlijk worden vastgelegd" is behaald gedurende de verslagperiode van dd/mm/jjjj tot dd/mm/jjjj.
Oordeel met beperking
Ons oordeel is gevormd op basis van de aangelegenheden die in de rapportages zijn uiteengezet. De criteria waarvan wij gebruik hebben gemaakt bij het vormen van ons oordeel zijn de criteria die in de vermelding van de XYZ serviceorganisatie op pagina [aa] staan beschreven. Naar ons oordeel, in alle van materieel belang zijnde aspecten, uitgezonderd de aangelegenheid die staat beschreven in de paragraaf 'Onderbouwing van het oordeel met beperking':
(a) … 13-21.]