NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Richtlijn 4401 Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie

Inleiding

1. Deze Richtlijn heeft ten doel grondslagen en essentiële werkzaamheden vast te stellen en aanwijzingen te geven omtrent de vaktechnische verantwoordelijkheid van de IT-auditor ten aanzien van de uitvoering van een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie, en omtrent de vorm en inhoud van het rapport dat de IT-auditor in het kader van een dergelijke opdracht uitbrengt.

1a. In de Richtlijnen hebben de volgende termen de hierna weergegeven betekenis:

- IT-auditor: de Register EDP-auditor (RE), ingeschreven in het register van de NOREA;
- IT-auditorganisatie: de naam van de organisatie, het organisatieonderdeel of rechstvorm waaronder de IT-auditor opereert c.q. de organisatie van meer IT-auditors;
- Opdrachtnemer: de IT-auditor of IT-auditorganisatie die de opdracht aanvaardt; hierna in deze richtlijn wordt – tenzij anders vermeld – uitsluitend gesproken van IT-auditor;
- Opdrachtgever: de partij of partijen die de opdracht verstrekt c.q. verstrekken;
- Opdracht: de professionele dienst bestaande uit het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie;
- Opdrachtbevestiging: de formele overeenkomst tussen opdrachtgever en opdrachtnemer ter bevestiging van de inhoud en reikwijdte van de opdracht;
- Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie: een opdracht waarbij de IT-auditor overeengekomen specifieke werkzaamheden verricht en hij hierover, zonder conclusies of aanbevelingen, de feitelijke bevindingen rapporteert. Gebruikers van het rapport zullen zich zelf een oordeel moeten vormen betreffende de werkzaamheden en bevindingen die door de IT-auditor in het rapport zijn weergegeven en hun eigen conclusies moeten trekken uit de door de IT-auditor verrichte werkzaamheden;

- Gebruikers: de opdrachtgever en met de opdrachtgever overeengekomen andere gebruikers of vertegenwoordigers hiervan, die in staat zijn zich een oordeel te vormen over de werkzaamheden en de bevindingen en hun eigen conclusies kunnen trekken.

2. Deze Richtlijn is van toepassing op opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie. Het is van belang dat eenduidigheid bestaat omtrent de aard en doel van de opdracht. Deze Richtlijn kan gebruikt worden in die situaties waarbij geen sprake is van een assurance-opdracht maar wel behoefte bestaat om al dan niet aan derden, over bepaalde aspecten te rapporteren op basis van met de opdrachtgever overeengekomen werkzaamheden. Aanwijzingen die in andere Richtlijnen zijn opgenomen kunnen voor de IT-auditor bij het toepassen van deze Richtlijn van dienst zijn.

2a.Deze Richtlijn kan worden toegepast op opdrachten met een rapportagedatum op of na 1 juli 2013.

3. Een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden omvat veelal het uitvoeren van bepaalde werkzaamheden met betrekking tot afzonderlijke aspecten van het object van onderzoek. Er vindt dan ten opzichte van een assurance-opdracht, een beperking plaats in de reikwijdte van het onderzoek.

Doel van de opdracht tot het verrichten van overeengekomen specifieke werkzaamheden

4. Het doel van een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie is het door de IT-auditor verrichten van die werkzaamheden die hij, de opdrachtgever en mogelijk andere gebruikers zijn overeengekomen en het rapporteren over de feitelijke bevindingen.

5. In het kader van een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden doet de IT-auditor uitsluitend verslag van de uitgevoerde werkzaamheden en de feitelijke bevindingen en geeft hij geen conclusie. Derhalve zullen de gebruikers van het rapport zelf een oordeel moeten vormen betreffende de werkzaamheden en bevindingen die door de IT-auditor in het rapport zijn weergegeven en zullen zij hun eigen conclusies moeten trekken uit de door de IT-auditor verrichte werkzaamheden.

5a Teneinde bij opdrachten tot overeengekomen specifieke werkzaamheden misverstanden te voorkomen op basis waarvan opdrachtgever of eventuele belanghebbenden zouden kunnen concluderen dat alsnog sprake is van een assurance opdracht, mogen geen woorden en/of symbolen[1] worden gebruikt waardoor de verwachting kan worden gewekt dat een assurance-opdracht wordt uitgevoerd waarmee een redelijke of beperkte mate van zekerheid, over het object van onderzoek, wordt verstrekt. Aanbevelingen, voor zover zij direct volgen vanuit de werkzaamheden, zullen ook niet in het rapport worden opgenomen, maar kunnen eventueel afzonderlijk worden gerapporteerd. Bij de planning, uitvoering en rapportering van de overeengekomen specifieke werkzaamheden vermijdt de IT-auditor daarom zoveel als mogelijk controle, beoordeling of toetsing (audit en review) gerelateerde woorden, mag de IT-auditor de termen beperkte en redelijke mate van zekerheid niet gebruiken en zal hij geen conclusies trekken of een waardering tot uitdrukking brengen.

6. Het rapport is uitsluitend bestemd voor gebruikers waarmee de te verrichten werkzaamheden zijn overeengekomen, aangezien anderen die niet op de hoogte zijn van het doel van de werkzaamheden, de resultaten onjuist kunnen interpreteren.

Algemene uitgangspunten inzake een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden

7. **De IT-auditor dient te voldoen aan de regelgeving zoals opgenomen in het Reglement Gedragscode (Code of Ethics)**. De beroepsregels stellen eisen aan de IT-auditor ten aanzien van:

[1] Bijvoorbeeld stoplichten en/of smileys

a. integriteit;

b. objectiviteit;

c. deskundigheid en zorgvuldigheid;

d. geheimhouding; en

e. professioneel gedrag.

Onafhankelijkheid betreft een nadere uitwerking van objectiviteit. Onafhankelijkheid is voor overeengekomen specifieke opdrachten geen vereiste, hoewel de voorwaarden voor de doelstelling van een opdracht als ook nationale voorschriften als eis kunnen stellen dat de IT-auditor voldoet aan de bepalingen van onafhankelijkheid. Ingeval de IT-auditor niet onafhankelijk is wordt dit feit in het Rapport van feitelijke bevindingen opgenomen.

8. **Indien deze richtlijn wordt toegepast dient de IT-auditor de opdracht tot het verrichten van overeengekomen specifieke werkzaamheden in overeenstemming met alle bepalingen van deze Richtlijn en met de voorwaarden van de opdracht uit te voeren.**

Vaststellen van de opdrachtvoorwaarden

9. **De IT-auditor dient er zeker van te zijn dat er met de opdrachtgever en eventuele andere gebruikers duidelijk overeenstemming bestaat over de overeengekomen werkzaamheden op basis van deze Richtlijn en met de opdrachtgever ook de overige voorwaarden van de opdracht**. Daarbij is het van belang om de inhoud, aard en omvang van de werkzaamheden in detail overeen te komen. De onderwerpen die in de opdrachtbevestiging onder meer aan de orde komen zijn:

- De aard van de opdracht en een verwijzing dat deze zal worden uitgevoerd met inachtneming van deze Richtlijn, dat derhalve de IT-auditor geen conclusie zal trekken en daarmee geen sprake is van een assurance-opdracht.
- De omschreven doelstelling van de opdracht.
- De aanduiding van het object van onderzoek waarop de overeengekomen specifieke werkzaamheden uitgevoerd zullen worden.
- De aard, de tijdsfasering en de omvang van de uit te voeren specifieke werkzaamheden.
- De te verwachten vorm van het rapport van feitelijke bevindingen.
- Beperkingen in de verspreiding van het rapport met de feitelijke bevindingen. Indien een dergelijke beperking in strijd is met wettelijke voorschriften accepteert de IT-auditor de opdracht niet.

9a. Het is de verantwoordelijkheid van de opdrachtgever en eventuele andere gebruikers om de specifieke werkzaamheden te bepalen. Bij het bepalen van de specifieke werkzaamheden kan de IT-auditor een adviserende rol vervullen, echter uiteindelijk dragen de opdrachtgever en de eventuele andere gebruikers de verantwoordelijkheid voor de overeengekomen specifieke werkzaamheden.

10. **De IT-auditor dient de te verrichten werkzaamheden met gebruikers die het rapport zullen ontvangen overeen te komen.** Dit kan door middel van het mee laten ondertekenen van de opdrachtbevestiging, maar de te verrichten werkzaamheden kunnen ook op andere wijze worden overeengekomen. Bij uitzondering zal onder bepaalde omstandigheden, bijvoorbeeld als de te verrichten werkzaamheden zijn vastgesteld door een regelgevende instantie, vertegenwoordigers uit de bedrijfstak en vertegenwoordigers van het IT-auditorsberoep, de IT-auditor niet in de gelegenheid zijn om de werkzaamheden met alle gebruikers die het rapport zullen ontvangen te bespreken. In dergelijke situaties kan de IT-auditor overwegen om bijvoorbeeld de uit te voeren werkzaamheden overeen te komen met de meest aangewezen vertegenwoordigers van de betrokken gebruikers, of de van belang zijnde correspondentie van betrokken gebruikers te beoordelen of deze gebruikers een ontwerp toe te zenden van het soort rapport dat uitgebracht zal worden.

10a. Met de opdrachtgever kan worden overeengekomen dat het rapport aan andere gebruikers dan de opdrachtgever kan worden verspreid. De IT-auditor vergewist zich ervan dat de ontvangende gebruiker in staat is zich een oordeel te vormen over de werkzaamheden en de bevindingen en zijn eigen conclusies kan trekken. Waar mogelijk houdt de IT-auditor in de formulering van zijn bevindingen rekening met de kennis, ervaring en achtergrond van de gebruiker.

11. Het is zowel in het belang van de opdrachtgever als van de IT-auditor dat de IT-auditor de opdrachtgever een bevestiging met de belangrijkste voorwaarden van de opdracht doet toekomen. Door middel van de opdrachtbevestiging wordt de acceptatie van de opdracht door de IT-auditor bevestigd. Tevens wordt met de opdrachtbevestiging beoogd misverstanden over de doelstelling en de reikwijdte van de opdracht, de omvang van de verantwoordelijkheid van de IT-auditor en de wijze van rapportering te voorkomen. NOREA Richtlijn 210 Opdrachtaanvaarding is onverkort van toepassing.

12. De onderwerpen die in aanvulling op het bepaalde in artikel 10 van NOREA Richtlijn 210 Opdrachtaanvaarding in de opdrachtbevestiging worden opgenomen zijn:

- Een opsomming van de uit te voeren werkzaamheden zoals die met gebruikers zijn overeengekomen.
- Een bepaling dat de verspreiding van het rapport van feitelijke bevindingen beperkt is tot de gebruikers met wie de uit te voeren werkzaamheden zijn overeengekomen.

Daarnaast kan de IT-auditor overwegen om een ontwerp van een rapport met feitelijke bevindingen aan de opdrachtbevestiging bij te voegen.

Planning

13. **De IT-auditor dient de werkzaamheden zodanig te plannen dat de opdracht doeltreffend wordt uitgevoerd.**

Documentatie

14. **De IT-auditor dient datgene vast te leggen wat van belang is voor de onderbouwing van het rapport van feitelijke bevindingen en voor het aantonen dat de opdracht is verricht in overeenstemming met deze Richtlijn en de voorwaarden van de opdracht.**
NOREA Richtlijn 230 Documentatie is onverkort van toepassing.

Uit te voeren werkzaamheden en onderbouwing

15. **De IT-auditor dient de overeengekomen specifieke werkzaamheden uit te voeren en de verkregen informatie als basis voor het rapport van feitelijke bevindingen te gebruiken.**

16. De werkzaamheden die in een opdracht van specifieke overeengekomen werkzaamheden worden toegepast bestaan onder meer uit:

- Het inwinnen van inlichtingen.
- Het observeren (van toestanden of activiteiten).
- Het inspecteren van documenten, rapportages, uitgeprinte en elektronische vastleggingen.
- Het herhalen van de uitvoering van de interne beheersingsmaatregelen.
- Het verkrijgen van bevestigingen van derden.

Rapportering

17. Het rapport omtrent overeengekomen specifieke werkzaamheden moet voldoende gedetailleerd een beschrijving van het doel en van de overeengekomen werkzaamheden geven, teneinde de lezer in staat te stellen de aard en de reikwijdte van de uitgevoerde werkzaamheden te begrijpen.

18. **Het rapport van feitelijke bevindingen dient te bevatten:**

a) **een opschrift dat duidelijk aangeeft dat dit een rapport van bevindingen betreft;**

b) **geadresseerde (dit zal doorgaans de opdrachtgever zijn die de IT-auditor heeft aangetrokken om de overeengekomen specifieke werkzaamheden uit te voeren);**

c) **identificatie van het object van onderzoek waarop de overeengekomen specifieke werkzaamheden toegepast zijn;**

d) **de vermelding dat de met de gebruiker overeengekomen werkzaamheden zijn uitgevoerd;**

e) **de vermelding dat de opdracht is uitgevoerd overeenkomstig NOREA Richtlijn 4401: 'Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden met betrekking tot informatietechnologie';**

f) **indien van toepassing, de vermelding dat de IT-auditor niet onafhankelijk van de opdrachtgever is;**

g) **de beschrijving van het doel waarvoor de overeengekomen specifieke werkzaamheden zijn uitgevoerd;**

h) **de beschrijving van de uitgevoerde specifieke werkzaamheden;**

i) **de beschrijving van de feitelijke bevindingen van de IT-auditor inclusief voldoende details van eventuele gevonden fouten en afwijkingen;**

j) **de vermelding dat geen assurance-opdracht is uitgevoerd en dat derhalve geen zekerheid over het object van onderzoek wordt verstrekt;**

k) **de vermelding dat indien de IT-auditor andere (aanvullende) werkzaamheden of een assurance-opdracht zou hebben uitgevoerd, wellicht andere onderwerpen zouden zijn geconstateerd en gerapporteerd;**

l) **de vermelding van de verspreidingskring en dat de verspreiding van het rapport is beperkt tot degenen met wie de uit te voeren werkzaamheden en/of verspreiding zijn overeengekomen;**

m) **datum van het rapport;**

n) **plaats van ondertekening door de IT-auditor; en**

o) **ondertekening (naam IT-auditor met vermelding naam IT-auditorganisatie)**.