|  |  |  |
| --- | --- | --- |
| **VK02** | **Vragenlijst Dossieronderzoek NOREA:****Assurance-opdrachten** | **Afstemming met lid CKO d.d.:** |
| **Naam IT-auditorganisatie:** | **Dossier:** | **Jaar:** |
| **Teamleider:** | **Onderzoeker:** | **Ingevuld d.d.:** |
| **INHOUDSOPGAVE** | **Artikel** |
| Inleiding | 1 |
| Opdrachtaanvaarding | 2 t/m 8 |
| Planning en uitvoering professionele dienst | 9 t/m 13 |
| Dossier | 14 t/m 18 |
| Rapportage | 19 t/m 22 |
| Conclusie | 23 t/m 26 |
| **Nummer** | **Omschrijving** | **Toelichting** |
| **INLEIDING** |
| 1. | **Gegevens opdracht** |
| * Omschrijving opdracht
 |  |
| * Aard van de assurance-opdracht
 |  |
| * Opdrachtgever
 |  |
| * Onderzoeksobject
 |  |
| * Verantwoordelijke partij onderzoeksobject
 |  |
| * Omvang opdracht
 | In Euro’s | € |
| Waarvan subcontractor | € |
| Aantal uren |  |
| Waarvan subcontractor |  |
| **Gegevens opdrachtteam** |
| * Eindverantwoordelijk IT-auditor
 |  |
| * Teamleden
 |  |
| **Toelichting op begrippen** |
| Bij de omschrijving van de opdrachtgever moet worden vermeld of sprake is van een nieuwe / bestaande klant, auditklant, interfirmsituatie, segment, nieuwe/herhaalde opdracht. Verder moet worden vermeld: risicoclassificatie cliënt én opdracht, gebruik van subcontractors, aantal uren besteed, rapportagedatum, omvang van de fee, lopende/gesloten opdracht, declaratieomvang, branche waarin de klant werkzaam is, soort huishouding, etc. |
| **Basis normering** |
| Het uitgangpunt voor het kwaliteitsonderzoek is het RKBN, het Stramien voor Assurance-opdrachten, Richtlijn 3000 A/D, Richtlijn 3402 en de NOREA Handreiking SOC2 en SOC3. De kwaliteitsonderzoeker wordt geacht deze te kennen. Het kwaliteitsonderzoek heeft tot doel te onderzoeken of het door de IT-auditorganisatie toegepaste kwaliteitsstelsel voldoet aan het RKBN, de Statuten, Reglementen en Richtlijnen van NOREA, mede aan de hand van een deelwaarneming op opdrachtdossiers. |

| **Nr.** | **Omschrijving** | **Ja/Nee/nvt** | **Toelichting** |
| --- | --- | --- | --- |
| **OPDRACHTAANVAARDING** |
| 2. | [RKBN, art. 12a]De IT-auditorganisatie heeft de integriteit van de opdrachtgever beoordeeld.  | Ja/Nee/nvt |  |
| 3. | [RKBN, art. 12b]De IT-auditorganisatie heeft een afweging gemaakt of zij de deskundigheid bezit om de professionele dienst uit te voeren en de capaciteiten, tijd en middelen daartoe bezit. | Ja/Nee/nvt |  |
| 4. | [RKBN, art. 12c] en [Code of Ethics, art. 100.5 T1]De IT-auditorganisatie heeft vastgesteld dat voldaan wordt aan de ethische normen, waaronder de vraag of door het accepteren van een opdracht van een nieuwe of bestaande opdrachtgever een belangenverstrengeling in wezen of schijn kan ontstaan. Let hierbij op de vereisten, aangeduid met de letter ‘V’ in de Code of Ethics.Van belang is ook (de verantwoordelijke voor) het onderzoeksobject en de onafhankelijkheid van de IT-auditorganisatie ten opzichte daarvan. | Ja/Nee/nvt |  |
| 5. | [RKBN, art. 15] en [Reglement Gedragscode art. 900.11]De IT-auditorganisatie heeft de verantwoordelijkheid voor de professionele dienst opgedragen aan een voor de opdrachtverantwoordelijk IT-auditor en daarbij vastgesteld dat deze over de juiste deskundigheid, capaciteiten, bekwaamheden, bevoegdheid en gezag beschikt en voldoende tijd heeft om zijn taak uit te voeren.Daarbij dient de onafhankelijkheid van de opdrachtgever\opdracht voor zowel de opdrachtverantwoordelijke IT-auditor en het gehele Audit Team tot uiting te komen in een verklaring. | Ja/Nee/nvt |  |
| 6. | [Richtlijn 210, art 9 en 10] en [Richtlijn 3000, art. 27]De opdrachtvoorwaarden zijn vastgelegd in een schriftelijke opdrachtbevestiging (of een andere geschikte vorm van een overeenkomst), die voldoet aan de daaraan te stellen eisen:a. Het doel van de opdracht.b. De verantwoordelijkheden van de IT-auditorc. De verantwoordelijkheden van de opdrachtgever.d. De reikwijdte (scope) van de opdracht.e. De wijze van rapportering en andere vormen van communicatie over de bevindingen inzake de opdracht, voor zover van toepassing.f. De waarborg voor de vrije toegang tot alle personen, informatiesystemen, vastleggingen, documentatie en andere informatie die in het kader van de opdracht wordt gevraagd.g. De wijze waarop het honorarium wordt vastgesteld en afspraken inzake het declareren, voor zover van toepassing.h. De afspraken over de planning.i. Een verzoek aan de opdrachtgever de acceptatie van de op-drachtvoorwaarden te bevestigen door het terugsturen van een getekend exemplaar van de opdrachtbevestiging. | Ja/Nee/nvt |  |
| 7. | Tussentijdse wijzigingen in de opdracht en de opdrachtvoorwaarden zijn eveneens schriftelijk vastgelegd en voor akkoord bevestigd door de opdrachtgever. | Ja/Nee/nvt |  |
| 8. | Heeft een ‘Richtlijn 3402’-opdracht een reikwijdte die bij aanvaarding voldoende relevant is voor de interne beheersing van de gebruikersorganisatie in relatie tot de financiële verslaglegging?Heeft een ‘SOC2/SOC3’-opdracht een scope die aansluit met de Trust Services Criteria voor Security met daar mogelijk aan toegevoegd één of meerdere aanvullende toe te voegen ‘categories’?:* Availabilty;
* Processing integrity;
* Confidentiality;
* Privacy.
 | Ja/Nee/nvt |  |
| **PLANNING EN UITVOERING PROFESSIONELE DIENST** |
| 9. | De opdracht is adequaat gepland. Hierbij is door de IT-Auditorganisatie voldoende aandacht besteed aan de waarborgen in het kwaliteitsstelsel om te voldoen aan het RKBN, de Statuten, Reglementen en Richtlijnen van NOREA. | Ja/Nee/nvt |  |
| 10. | Bij het opstellen van de planning is:* afdoende kennis over het onderzoeksobject [3000 art 24] en
* overige omstandigheden bij de opdracht [3000 art 24, 25, 28,30, 37,43, 46B, 46R] verkregen om de risico's van onjuistheden van materieel belang in de informatie over het onderzoeksobject te signaleren en te beoordelen; tevens
* de procedure voor het verzamelen van (assurance) informatie [3000 art 10, 12, 23, 24, 29, 33, 50] opgesteld en uitgevoerd.
* de desbetreffende richtlijn gevolgd [3000 art 40].
 | Ja/Nee/nvt |  |
| 11. | De op de opdracht van toepassing zijnde criteria zijn bij: * attest (3000A): kader komt van opdrachtgever/systeemverantwoordelijke, en auditor moet onderzoeken of het toereikend is.
* directe opdracht (3000D): auditor stelt kader op, opdrachtgever accordeert.

Heeft de auditor het normenkader beoordeeld op geschiktheid ten behoeve van het evalueren of het toetsen van het onderzoeksobject. | Ja/Nee/nvt |  |
| 12. | [3000 Art. 12f]Bij de planning en de uitvoering van de opdracht is rekening gehouden met het materieel belang (factoren die beslissingen van de beoogde gebruikers van het assurance rapport beïnvloeden) en het opdrachtrisico. | Ja/Nee/nvt |  |
| 13. | [3000 Art. 32, 52]Indien bij het verzamelen en het evalueren van (assurance) informatie gebruik is gemaakt van de werkzaamheden van een deskundige, is vastgesteld dat deze beschikt over adequate kennis en ervaring met betrekking tot het onderzoeksobject en de van toepassing zijnde criteria, zodat het opdrachtteam kan vaststellen dat voldoende (assurance) informatie is verkregen. | Ja/Nee/nvt |  |
| **DOSSIER** |
| 14. | [RKBN, art. 33]Uit het dossier blijkt dat de door de IT-auditorganisatie voorgeschreven procedures voor kwaliteitsbeheersing, die gericht zijn op de verantwoordelijkheid van allen die de opdracht uitvoeren, zijn uitgevoerd. | Ja/Nee/nvt |  |
| 15. | [RKBN, art. 15, 16, 17]Het dossier bevat een adequate vastlegging waaruit blijkt dat de geplande werkzaamheden, zijn uitgevoerd conform de desbetreffende richtlijn en dat de voor de professionele dienst verantwoordelijk IT-auditor in alle fasen van de opdracht in voldoende mate betrokken is geweest. | Ja/Nee/nvt |  |
| 16. | [3000, Art. 66, 79 en [230, Art. 8]Het dossier bevat alle verkregen (assurance) informatie die van betekenis is voor de onderbouwing van het Assurance rapport. | Ja/Nee/nvt |  |
| 17. | [3000, Art. 36]Het dossier bevat een vastlegging van de overwegingen aangaande alle aspecten die een vakkundige oordeelsvorming vereisen en van de conclusies die daaruit zijn getrokken. | Ja/Nee/nvt |  |
| 18 | [3000, Art. 56-59]Het dossier bevat schriftelijke bevestigingen van de verantwoordelijke partij(en) die voldoen aan de eisen uit de richtlijn. | Ja/Nee/nvt |  |
| **RAPPORTAGE** |
| 19. | [3000, Art. 67 en 68]Het Assurance rapport is schriftelijk uitgebracht en bevat een duidelijke formulering van de conclusie over de informatie betreffende het onderzoeksobject en voldoet aan de in de desbetreffende richtlijn vastgestelde onderdelen en criteria (en indien van toepassing aan de aanwijzingen uit de Handreiking SOC2/SOC3).Hierbij hoort dat een objectieve, redelijk en geïnformeerde (derde partij) toets is uitgevoerd op de relatie tussen bevindingen en oordeel/conclusie (audit-trail). | Ja/Nee/nvt |  |
| 20. | [3000, Art. 69] en [3402 Art. 53]Het rapport bevat de minimaal voorgeschreven basiselementen voor een Assurance rapport zoals in de desbetreffende richtlijn zijn voorgeschreven. Samengevat betreft dat: **(a)** Een titel die duidelijk aangeeft dat de rapportage een Assurance-rapport is van een onafhankelijke IT-auditor. **(b)** Een geadresseerde. **(c)** Identificatie of beschrijving van het niveau van zekerheid dat door de IT-auditor is verkregen, de informatie over het onderzoeksobject of, wanneer van toepassing, het onderzoeksobject zelf..**(d)** Aanduiding van de van toepassing zijnde criteria en de partij die de interne beheersingsdoelstellingen specificeert. **(e)** Waar passend, een beschrijving van significante inherente beperkingen die verband houden met de meting of evaluatie van het onderzoeksobject ten opzichte van de van toepassing zijnde criteria..**(f)** Wanneer de van toepassing zijnde criteria voor een bepaald doel zijn ontworpen, een vermelding van het feit dat de informatie over het onderzoeksobject mogelijk niet geschikt is voor een ander doel.**(g)** Een vermelding dat de verantwoordelijkheid van de IT-auditor van de serviceorganisatie. **(h)** Een vermelding dat de IT-auditeenheid waarbij de IT-auditor werkzaam is of aan verbonden is, de (specifieke) Richtlijn heeft toegepast.**(i)** Een vermelding dat de IT-auditor de vereisten van het RKBN en heeft nageleefd.**(j)** Een vermelding dat de opdracht overeenkomstig de Code of Ethics is uitgevoerd. **(k)** Een samenvatting van de uitgevoerde werkzaamheden van de IT-auditor van de serviceorganisatie. **(l)** Het oordeel of de conclusie van de IT-auditor van de serviceorganisatie Een vermelding van de beperkingen van interne beheersingsmaatregelen en, indien van toepassing, de projectie naar toekomstige verslagperiodes. **(m)** Handtekening van de IT-auditor.**(n)** Datum van het assurance-rapport. | Ja/Nee/nvt |  |
| 21. | [RKBN, art. 18]Voor zover in het kader van de opdracht consultatie heeft plaatsgevonden, zijn de eindoordelen voortkomend uit de consultatie in het dossier vastgelegd en in het rapport overgenomen. | Ja/Nee/nvt |  |
| 22. | [RKBN, art. 21]Voor zover de opdracht volgens de procedures van de IT-auditorganisatie daartoe in aanmerking komt, heeft een opdrachtgerichte kwaliteitsbeoordeling plaatsgevonden voordat het rapport is uitgebracht. | Ja/Nee/nvt |  |
| **CONCLUSIE VAN DE KWALITEITSONDERZOEKER** |
| 23. | Luidt op grond van de bevindingen van de kwaliteitsonderzoeker dat de in het dossier weergegeven uitgevoerde werkzaamheden een deugdelijke grondslag vormen voor de rapportage? | Ja/Nee/nvt |  |
| 24. | Luidt op grond van de in het opdrachtdossier vastgelegde bevindingen dat de rapportage geen belangrijke onjuistheden of onvolkomenheden bevat? | Ja/Nee/nvt |  |
| 25. | Luidt op grond van de bevindingen van de kwaliteitsonderzoeker dat een juiste rapportage heeft plaatsgevonden? | Ja/Nee/nvt |  |
| 26. | Geef de conclusie over het onderzochte dossier, inclusief motivatie, ten aanzien van de toepassing van het kwaliteitsstelsel. |  |