| **B4.4** | | **Vragenlijst Dossierreview NOREA** | | **Beoordeeld lid CKO d.d.** | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Naam IT-auditorganisatie:** | | | | | **Dossier:** | | | **2019** |
| **Teamleider:** | | | **Onderzoeker:** | **Ingevuld** | | | | |
| **INHOUDSOPGAVE** | | | | | | | **Artikel** | |
| Inleiding | | | | | | | 1 | |
| Opdrachtaanvaarding | | | | | | | 2 t/m 7 | |
| Planning en uitvoering professionele dienst | | | | | | | 8 t/m 12 | |
| Dossier | | | | | | | 13 t/m 16 | |
| Rapportage | | | | | | | 17 t/m 20 | |
| Eindoordeel | | | | | | | 21 t/m 24 | |
| **Artikel** | **Omschrijving** | | | **Ja/nee/nvt** | | **Evidence/opmerking** | | |
|  | | **INLEIDING** | | | | | | |
| 1. | | **Gegevens opdracht** | | | | | | |
| * Omschrijving opdracht | |  | | | | |
| * Opdrachtgever | |  | | | | |
| * Omvang opdracht | | In € | |  | | |
| Waarvan subcontractor | | € | | |
| Aantal uren | | **]** | | |
| Waarvan subcontractor | |  | | |
| **Gegevens opdrachtteam** | | | | | | |
| * Eindverantwoordelijke IT-auditor | |  | | | | |
| * Teamleden | |  | | | | |
| **Toelichting op begrippen** | | | | | | |
| 1. Bij de omschrijving van de opdracht moet onderscheid worden gemaakt tussen assurance- en non-assurance-opdrachten. De opdrachten moeten, voor zover mogelijk, nader worden geïdentificeerd (audit, review, overeengekomen specifieke werkzaamheden, advies, detachering, product, Internal Audit Support, Risk Management, wederkerende opdracht, etc.) | | | | | | |
| 2. Bij de omschrijving van de opdrachtgever moet worden vermeld of sprake is van een nieuwe / bestaande klant, audit klant, inter-firm situatie, segment, nieuwe/herhaalde opdracht. Verder moet worden vermeld: risicoclassificatie cliënt en 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** | | | | | | |
| In deze vragenlijst wordt per norm zoveel mogelijk verwezen naar de onderliggende regelgeving, in het bijzonder het RKBN, Norea Richtlijn 3000, 3402, handreiking SOC2 en DigiD-Assessments. Deze richtlijnen hebben betrekking op Assurance opdrachten. In het geval de opdracht géén assurance-opdracht betreft, dient het review team zelf na te gaan of de betreffende norm in meer of mindere mate op de opdracht van toepassing is. | | | | | | |
| **Ingangsdatum** | | | | | | |
| Deze vragenlijst treedt in werking op 1 mei 2017  **Zie voor overstijgende informatie het RKBN.** | | | | | | |
|  | | **OPDRACHTAANVAARDING** | | | | | | |
| 2. | | De IT-auditorganisatie heeft de integriteit van de opdrachtgever beoordeeld | | Ja/nee/nvt | |  | | |
| 3. | | 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. | | 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 belangentegenstelling in wezen of schijn kan ontstaan. | | Ja/nee/nvt | |  | | |
| 5. | | De IT-auditorganisatie heeft de verantwoordelijkheid voor de professionele dienst opgedragen aan een voor de opdracht verantwoordelijke professional en daarbij vastgesteld dat deze over de juiste capaciteiten, bekwaamheden, bevoegdheid en het gezag beschikt en voldoende tijd heeft om zijn taak uit te voeren | | Ja/nee/nvt | |  | | |
| 6. | | De opdrachtvoorwaarden zijn vastgelegd in een opdrachtbevestiging (of een andere geschikte vorm van een overeenkomst), die voldoet aan de daaraan te stellen eisen. Moet in lijn zijn met de Norea richtlijn 3000 3402, handreiking SOC2 en DigiD-Assessments. | | Ja/nee/nvt | |  | | |
| 7. | | Wijzigingen in de opdracht en de opdrachtvoorwaarden zijn eveneens schriftelijk vastgelegd en voor akkoord getekend door de opdrachtgever | | Ja/nee/nvt | |  | | |
|  | | **PLANNING EN UITVOERING PROFESSIONELE DIENST** | | | | | | |
| 8. | | De opdracht is adequaat gepland. Hierbij is voldoende aandacht besteed aan het ontwikkelen van een algehele strategie voor de reikwijdte, de diepgang, het tijdschema en de uitvoering van de opdracht, en het ontwikkelen van de detailplanning van de opdracht, bestaande uit een gedetailleerde aanpak voor aard, tijdsfasering en omvang van de procedures die moeten worden uitgevoerd om (assurance) informatie te verzamelen en de onderbouwing voor de keuze daarvan | | Ja/nee/nvt | |  | | |
| 9. | | In het kader van de planning is afdoende kennis over het object van onderzoek en andere omstandigheden rond de opdracht verkregen om de risico's van onjuistheden van materieel belang in de informatie over het object van onderzoek te signaleren en te beoordelen en tevens de procedures voor het verzamelen van (assurance) informatie op te stellen en uit te voeren | | Ja/nee/nvt | |  | | |
| 10. | | De op de opdracht van toepassing zijnde criteria zijn vastgelegd in een door de opdrachtgever geaccordeerd normenkader en beoordeeld op toepasbaarheid ten behoeve van het evalueren of het toetsen van het object van onderzoek | | Ja/nee/nvt | |  | | |
| 11. | | Bij de planning en de uitvoering van de opdracht is rekening gehouden met het materieel belang (factoren die beslissingen van de beoogde gebruikers beïnvloeden) en het opdrachtrisico. | | Ja/nee/nvt | |  | | |
| 12. | | 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 object van onderzoek en de van toepassing zijnde criteria, zodat de beroepsbeoefenaar kan vaststellen dat voldoende (assurance) informatie is verkregen | | Ja/nee/nvt | |  | | |
|  | | **DOSSIER** | | | | | | |
| 13. | | 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 | |  | | |
| 14. | | Het dossier bevat een adequate vastlegging waaruit blijkt dat de geplande werkzaamheden zijn uitgevoerd en dat voor de professionele dienst verantwoordelijke in alle fasen van het onderzoek in voldoende mate betrokken is geweest | | Ja/nee/nvt | |  | | |
| 15. | | Het dossier bevat alle verkregen (assurance) informatie die van betekenis is voor de onderbouwing van de eindrapportage (assurance- of adviesrapport) | | Ja/nee/nvt | |  | | |
| 16. | | 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 | |  | | |
|  | | **RAPPORTAGE** | | | | | | |
| 17. | | Het rapport is schriftelijk uitgebracht en bevat een duidelijke formulering van de conclusie over de informatie betreffende het object van onderzoek dan wel een duidelijke formulering van het uitgebrachte advies | | Ja/nee/nvt | |  | | |
| 18. | | Indien sprake is van een assurance opdracht, bevat het rapport de minimaal voorgeschreven basiselementen voor een assurance-rapport – conform Norea Richtlijn 3000, 3402, handreiking SOC2 en DigiD-Assessments. | | Ja/nee/nvt | |  | | |
| 19. | | 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 | |  | | |
| 20. | | 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 | |  | | |
|  | | **EINDOORDEEL** | | | | | | |
| 21. | | Luidt op grond van de bevindingen dat de in het dossier weergegeven uitgevoerde werkzaamheden een deugdelijke grondslag vormen voor de rapportering? | | Ja/nee/nvt | |  | | |
| 22. | | Luidt op grond van de in het dossier vastgelegde bevindingen dat de rapportering geen belangrijke onjuistheden of onvolkomenheden bevat? | | Ja/nee/nvt | |  | | |
| 23. | | Luidt op grond van de bevindingen dat een juiste rapportering heeft plaatsgevonden? | | Ja/nee/nvt | |  | | |
| 24. | | Geef het eindoordeel over het getoetste dossier, inclusief motivatie | |  | |  | | |

**Eigen toevoeging – uitwerking artikel 18**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Inhoud van het rapport (NOREA 3000A)** | | **Handboek organidastie** | **Rapport geselecteerd dossier** | **verschil** |
|  | Een titel die duidelijk aangeeft dat het rapport een onafhankelijk assurance-rapport betreft. |  |  |  |
|  | Een geadresseerde. |  |  |  |
|  | Een beschrijving van de doelstelling van de opdracht |  |  |  |
|  | Een identificatie of beschrijving van het niveau van zekerheid dat door de IT-auditor is verkregen en een beschrijving over het onderzoeksobject zelf |  |  |  |
|  | Beschrijving van de van toepassing zijnde criteria. |  |  |  |
|  | 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. |  |  |  |
|  | Wanneer de van toepassing zijnde criteria voor een bepaald doel zijn ontworpen, een vermelding die lezers hierop attent maakt en op het feit dat, als gevolg hiervan, het onderzoeksobject mogelijk niet geschikt is voor een ander doel. |  |  |  |
|  | Een vermelding van de verantwoordelijke partij alsmede een omschrijving van hun verantwoordelijkheden en die van de ITauditor. |  |  |  |
|  | Een vermelding dat de opdracht overeenkomstig deze Richtlijn is uitgevoerd, of waar er een specifieke Richtlijn voor het onderzoeksobject is, die Richtlijn. |  |  |  |
|  | Een vermelding dat de IT-audit-eenheid waarbij de IT-auditor werkzaam is of aan verbonden is, het Reglement Kwaliteitsbeheersing NOREA (RKBN) of regelgeving die ten minste gelijkwaardig is, toepast. Indien de eindverantwoordelijk professional geen IT-auditor is, dient de vermelding de professionele vereisten te identificeren die zijn toegepast. |  |  |  |
|  | Een vermelding dat de IT-auditor de vereisten van het Reglement Gedragscode ('Code of Ethics') heeft nageleefd. Als de eindverantwoordelijk professional geen IT-auditor is, dient de vermelding de vergelijkbare professionele vereisten te identificeren die zijn toegepast. |  |  |  |
|  | Een informatieve samenvatting van de uitgevoerde werkzaamheden als basis voor de conclusie van de IT-auditor. In het geval van een directe-opdracht, is een begrip van de aard, timing en omvang van de uitgevoerde werkzaamheden essentieel voor het inzicht in de conclusie van de IT-auditor.  Bij een opdracht met een beperkte mate van zekerheid dient de samenvatting van de uitgevoerde werkzaamheden het volgende te vermelden:   1. Dat de werkzaamheden die bij een opdracht met een beperkte mate van zekerheid zijn uitgevoerd verschillend zijn in aard en timing en geringer van omvang zijn dan voor opdrachten tot het verkrijgen van een redelijke mate van zekerheid; en 2. Dat daardoor het niveau van zekerheid dat is verkregen bij een opdracht met een beperkte mate van zekerheid aanzienlijk lager ligt dan wanneer een opdracht met een redelijke mate van zekerheid was uitgevoerd. |  |  |  |
|  | De conclusie van de IT-auditor:   1. Wanneer dit passend is, dient de conclusie de beoogde gebruikers te informeren over de context waarin de conclusie van de IT-auditor moet worden gelezen. 2. Bij een opdracht met een redelijke mate van zekerheid dient de conclusie in bevestigende vorm te worden geformuleerd. 3. Bij een opdracht met een beperkte mate van zekerheid dient de conclusie tot uitdrukking te worden gebracht in een vorm die, op basis van de uitgevoerde werkzaamheden en de verkregen assurance-informatie, uitdrukt of er een aangelegenheid onder de aandacht van de IT-auditor is gekomen die ertoe leidt dat hij veronderstelt dat het onderzoeksobject een verschil van materieel belang bevat. 4. De conclusie in (ii) of (iii) dient te worden geformuleerd door gebruik te maken van de gepaste bewoordingen voor het onderzoeksobject en de van toepassing zijnde criteria gezien de omstandigheden van de opdracht. 5. Wanneer de IT-auditor een aangepaste conclusie formuleert, dient het assurance-rapport het volgende te bevatten: 6. Een sectie die een beschrijving geeft van de aangelegenheid die tot de aanpassing heeft geleid; en 7. Een sectie die de aangepaste conclusie van de IT-auditor bevat. |  |  |  |
|  | De handtekening van de IT-auditor. |  |  |  |
|  | De datum van het assurance-rapport. Het assurance-rapport dient niet te worden gedateerd vóór de datum waarop de IT-auditor de assurance-informatie heeft verkregen waarop hij zijn conclusie heeft gebaseerd. Hieronder valt tevens de ontvangst van de schriftelijke bevestigingen onder de paragrafen 56 en 57. |  |  |  |
|  | De locatie in het rechtsgebied waar de IT-auditor werkzaam is. |  |  |  |