

Tweede nota van inlichtingen (selectiefase)

Nr.	Verwijzing (doc, art, par en/of vraag)	Pagina nummer	Vraag	Antwoord
1.	NVI-1 antwoord op vraag 2		De selectieleidraad bepaalt dat een SOC 2 Type II-assurance-rapportage of een daaraan gelijkwaardige onafhankelijke assurance-rapportage dient te worden overgelegd. In de Nota van Inlichtingen is verduidelijkt dat een ISO 27001-certificering in combinatie met een ISAE 3000 Type II-rapport, dat de werking van beveiligingscontroles over een aaneengesloten periode bevestigt, als gelijkwaardig alternatief wordt geaccepteerd. Leverancier beschikt over een ISAE 3402 Type II-verklaring in combinatie met een ISO 27001-certificering. Binnen deze assurance-opdracht beoordeelt een onafhankelijke externe auditor jaarlijks de opzet, het bestaan en de effectieve werking van vijftig beheersmaatregelen gedurende een aaneengesloten controleperiode. Deze beheersmaatregelen omvatten onder meer informatiebeveiliging, toegangsbeheer, wijzigingsbeheer, incidentmanagement, patchmanagement, security baselines, back-up en restore, monitoring, bedrijfscontinuïteit en fysieke beveiliging van het datacenter. De werking van deze beheersmaatregelen wordt gedurende de controleperiode onafhankelijk getoetst. Inschrijver begrijpt uit de beantwoording in de Nota van Inlichtingen dat de aanbestedende dienst een assurance-rapportage die de werking van beveiligingscontroles gedurende een aaneengesloten periode bevestigt, in combinatie met een ISO 27001-certificering, als gelijkwaardig alternatief voor een SOC 2 Type II aanmerkt. Gelet op de inhoud, scope en diepgang van de ISAE 3402 Type II-assurance-opdracht lijkt deze eveneens aan dit uitgangspunt te voldoen. Kan de aanbestedende dienst verduidelijken of een ISAE 3402 Type II-verklaring, in combinatie met een ISO 27001-certificering, eveneens als een daaraan gelijkwaardige onafhankelijke assurance-rapportage wordt aangemerkt, indien uit de scope van de assurance-opdracht blijkt dat de relevante informatiebeveiligingsmaatregelen gedurende een	Aanbestedende dienst is het met Gegadigde eens dat ISAE 3402 Type II-rapportage in combinatie met een ISO 27001-certificering mogelijk wel voldoet aan de gestelde geschiktheidseis, namelijk wanneer deze verder gaat dan de rapportage van financiële controls, waarin ISAE 3402 Type II-rapportage in aanleg op toeziet. Dit is echter alleen het geval als Gegadigde kan aantonen dat: • De rapportage zekerheid biedt over beheersingsdoelstellingen die naar aard en omvang aansluiten bij de doelstellingen van de gevraagde SOC 2 Type II- of ISAE 3000 Type II-rapportage; • De scope van de rapportage aansluit bij de aangeboden dienstverlening en de relevante risico's (waaronder toegangsbeheer, wijzigingsbeheer, incidentmanagement, patchmanagement, back-up/restore, monitoring, BCM en fysieke beveiliging); • Een onafhankelijke auditor opzet, bestaan én effectieve werking van deze maatregelen heeft getoetst; • Dit is gebeurd over een aaneengesloten periode vergelijkbaar met die van SOC 2 Type II of ISAE 3000 Type II. Het is aan Gegadigde om de gelijkwaardigheid aan te tonen en een toelichting daarop bij te voegen aan de Aanmelding. De gelijkwaardigheid wordt vervolgens beoordeeld door de Aanbestedende dienst.

Tweede nota van inlichtingen (selectiefase)

Nr.	Verwijzing (doc, art, par en/of vraag)	Pagina nummer	Vraag	Antwoord
			aaneengesloten periode onafhankelijk zijn getoetst op de opzet, het bestaan en de effectieve werking?	
2.	NVI-1 antwoord op vraag 2		Inschrijver constateert dat het aantal marktpartijen dat beschikt over een SOC 2 Type II-rapportage dan wel een ISAE 3000 Type II-rapportage in combinatie met een ISO 27001-certificering beperkt is. Kan de aanbestedende dienst, mede gelet op het proportionaliteitsbeginsel en het belang van voldoende mededinging, bevestigen dat ook andere onafhankelijke assurance-rapportages die aantoonbaar een gelijkwaardig niveau van zekerheid bieden over de opzet, het bestaan en de effectieve werking van de relevante informatiebeveiligingsmaatregelen, zoals bedoeld in de selectieleidraad, voor acceptatie in aanmerking kunnen komen?	Aanbestedende dienst is zich bewust van de huidige situatie in de markt en de noodzaak voor een evenwichtige, inhoudelijke beoordeling van de bewijsvoering ten aanzien van deze eis. Zie in dit kader het antwoord op vraag 1 in deze tweede nota van inlichtingen.
3.	Nvl-en 1 vraag 14	6	Uw antwoord lijkt onvolledig, kunt u dit verder aanvullen?	In het kader van deze selectiefase gebruikt Inschrijver hiervoor het Uniform Europees Aanbestedingsdocument dat is aangemaakt in TenderNed en onder Aanbestedingsdocumentatie is gepubliceerd. Hiertoe kan deel II D worden voorzien van de gevraagde informatie en overlegt Gegadigde van iedere onderaannemer separaat een ingevuld UEA en tijdens de verificatiefase een gedragsverklaring aanbesteden.
4.	Nvl-en 1 vraag 7	3	Moeten Oracle en SQL databases als dienst binnen 1 referentie zijn of mag dit op twee referenties betrekking hebben?	Binnen één (1) referentie, zie ook paragraaf 8.2, selectie criterium 1: <i>Één (1) ingediende referentie -niet ouder van vijf (5) jaar, gerekend vanaf de publicatiedatum van deze concurrentie gerichte dialoog.</i> Zie in dit kader tevens het antwoord op vraag 13 in de nota van inlichtingen (selectiefase).
5.	Nvl-en 1 vraag 19	7	Kan aanbestedende dienst bevestigen of de één ingediende referentie voor Selectie criterium 1 tevens kan dienen als een van de referenties ter onderbouwing van de geschiktheidseisen	Gegadigde mag één (1) en dezelfde referentie indienen voor geschiktheidseis in paragraaf 6.2 en selectie criterium 1 in paragraaf 8.2 van de selectieleidraad.

Tweede nota van inlichtingen (selectiefase)

Nr.	Verwijzing (doc, art, par en/of vraag)	Pagina nummer	Vraag	Antwoord
			(paragraaf 6.2), of dient dit een separate/aanvullende referentie te zijn?	
6.	Nvl-en vraag 5 en 23	2 en 8	Deze antwoorden lijken niet consistent met elkaar. Kan aanbestedende dienst bevestigen of de fatale datum van 1 juli 2027 uitsluitend betrekking heeft op het beschikbaar en getest zijn van de landing zone (zoals omschreven in het antwoord op vraag 5), of dient op die datum tevens de volledige migratie van virtuele machines te zijn afgerond?	In het antwoord op vraag 23 in de nota van inlichtingen (selectiefase) stelt Aanbestedende dienst dat migratie <i>idealiter</i> op de genoemde data is uitgevoerd (en dat is nog steeds zo). Echter, uit het antwoord op vraag 5 in de nota van inlichtingen (selectiefase) blijkt dat Aanbestedende dienst zich realiseert dat dit lastig(er) haalbaar is vanwege de opgelopen vertraging in het aanbestedingsproces en dat alternatieve benaderingswijzen/planningen (in de concurrentiegericht dialog) bespreekbaar zijn.
7.	Nota van Inlichtingen, antwoord op vraag 35	12	Het is onduidelijk waarom de uitkering van de verzekering beperkt dient te zijn tot maximaal twee gebeurtenissen per jaar. Kan aanbestedende dienst bevestigen dat hier bedoeld wordt dat gegadigde dient te beschikken over een bedrijfsaansprakelijkheids-verzekering met minimaal een dekking van € 2.500.000,00 per gebeurtenis en minimaal een dekking van € 5.000.000,00 per jaar? Mocht dit niet correct zijn, kan aanbestedende dienst de eis dan nader toelichten?	Aanbestedende dienst bevestigt deze aanname.
8.	Nota van Inlichtingen, antwoord op vragen 2, 10 en 77	1,4 en 20	Vraag over gelijkwaardigheid van het control framework: In de beantwoording van vragen 2 en 10 geeft de aanbestedende dienst aan dat een ISAE 3402 Type II-rapportage niet als gelijkwaardig alternatief voor een SOC 2 Type II wordt geaccepteerd, omdat deze zich uitsluitend richt op financiële processen. Gegadigde merkt op dat de scope van een ISAE 3402 Type II-rapportage niet uitsluitend wordt bepaald door de standaard zelf, maar door het onderliggende Risk Control Framework en de processen waarop de audit betrekking heeft. In het geval van Gegadigde is de rapportage specifiek ingericht op de beheersing	Zie het antwoord op vraag 1 in deze tweede nota van inlichtingen.

Tweede nota van inlichtingen (selectiefase)

Nr.	Verwijzing (doc, art, par en/of vraag)	Pagina nummer	Vraag	Antwoord
			van operationele IT-dienstverlening, waaronder continuïteit, beschikbaarheid, logische en fysieke toegangsbeveiliging, wijzigingsbeheer, back-up- en herstelprocessen en informatiebeveiliging. Deze rapportage wordt bovendien ondersteund door ISO 27001-certificering, inclusief ISO 27017 certificering voor cloudbeveiliging en BIO 2.0 aantekening. Kan de Aanbestedende Dienst bevestigen dat een ISAE 3402 Type II-rapportage in combinatie met voornoemde certificeringen als gelijkwaardig alternatief wordt geaccepteerd indien de Gegadigde kan aantonen dat de geteste beheersingsmaatregelen en assurance-doelstellingen inhoudelijk dezelfde beveiligings- en continuïteitsrisico's adresseren als de gevraagde SOC 2 Type II of een ISAE 3000 Type II-rapportage i.c.m. een ISO27001 certificering, dan wel te motiveren waarom deze combinatie niet gelijkwaardig zou zijn? Aanvullend – methodologische gelijkwaardigheid en praktijktoepassing De combinatie van een ISAE Type II-verklaring, ISO 27001-certificering (inclusief ISO 27017-certificering) en aantoonbare BIO 2.0-conformiteit voldoet ruimschoots aan de DigiD-aansluitseisen en de daaraan verbonden toezicht- en verantwoordingsvereisten van Logius. Deze combinatie wordt reeds toegepast binnen een grootschalige private-cloudomgeving van een opdrachtgever van Gegadigde die kritieke dienstverlening aan lokale overheden levert, inclusief de opslag van persoonsgegevens, en wordt periodiek en onafhankelijk getoetst op de effectieve werking van de onderliggende beveiligings- en beheersingsmaatregelen.	

Tweede nota van inlichtingen (selectiefase)

Nr.	Verwijzing (doc, art, par en/of vraag)	Pagina nummer	Vraag	Antwoord
			Gelet op: • de toepassing van een specifiek op operationele IT-dienstverlening gericht Risk & Control Framework; • de methodologische grondslag binnen het internationaal erkende ISAE 3000-assurance-raamwerk; • de aanvullende certificeringen voor informatiebeveiliging en cloudbeveiliging; • de aantoonbare toepasbaarheid van deze assurance-combinatie binnen een door Logius beoordeelde omgeving voor kritieke dienstverlening aan lokale overheden; en • het feit dat de onderliggende beheersingsmaatregelen, auditmethodiek en assurance-doelstellingen materieel dezelfde informatiebeveiligings-, continuïteits- en beheersingsrisico's adresseren als de gevraagde assurance-vormen, verzoekt Gegadigde de Aanbestedende Dienst alsnog te bevestigen dat deze combinatie van assurance-rapportages en certificeringen als een gelijkwaardige vorm van zekerheid wordt beoordeeld ten opzichte van de gevraagde SOC 2 Type II-rapportage dan wel een ISAE 3000 Type II-rapportage in combinatie met een ISO 27001-certificering. Indien de Aanbestedende Dienst alsnog van oordeel is dat van gelijkwaardigheid geen sprake is, verzoekt Gegadigde de inhoudelijke, objectief toetsbare en proportionele gronden daarvoor nader te motiveren. Dit mede in het licht van de aanbestedingsrechtelijke beginselen van gelijkwaardigheid, proportionaliteit en objectieve toetsbaarheid, op grond waarvan niet uitsluitend de benaming van een certificering of assurance-rapportage, maar juist de	

Tweede nota van inlichtingen (selectiefase)

Nr.	Verwijzing (doc, art, par en/of vraag)	Pagina nummer	Vraag	Antwoord
			inhoudelijke dekking, de gehanteerde auditmethodiek, de assurance-doelstellingen en de aantoonbare werking van de onderliggende beheersmaatregelen bepalend dienen te zijn voor de beoordeling van gelijkwaardigheid.	