

Nummer	Paragraaf/artikel	Vraag	Antwoord
1	NVI 1 vraag 98 en 119	"Wij begrijpen het belang dat u hecht aan het waarborgen van de informatieveiligheid en transparantie bij de levering van kritische applicaties. In het Programma van Eisen stelt u echter als eis dat inschrijvers jaarlijks een ISAE 3402 of SOC 1 Type II rapport moeten overleggen. Wij verzoeken u deze eis nader te onderbouwen in het licht van de volgende overwegingen: 1) Artikel 35 van de GIBIT bepaalt dat een derdenverklaring (TPM), geldige ISO-certificering, of een vergelijkbaar kwaliteitssysteem, opgesteld door een register EDP-auditor of onafhankelijke deskundige, toereikend is om de kwaliteit van processen en beveiligingsmaatregelen aan te tonen. Uw eis van uitsluitend een ISAE 3402 of SOC 1 Type II rapport lijkt hiermee in tegenspraak te zijn. 2) De BIO, hoofdstuk 4.4, vereist dat de aanbestedende dienst inschrijvers vraagt een GAP-analyse en een Statement of Compliance op te leveren ten opzichte van de geselecteerde BIO-eisen. Dit biedt een breed spectrum aan beveiligingsmaatregelen, waarmee de exclusieve eis van een ISAE 3402 of SOC 1 Type II rapport mogelijk disproportioneel is. 3) In Advies 689 van de Commissie van Aanbestedingsexperts (4 september 2023) wordt expliciet benadrukt dat proportionaliteit in aanbestedingen vereist dat gestelde eisen in verhouding staan tot het doel van de opdracht en de lasten voor inschrijvers. Het advies stelt dat een aanbestedende dienst geen specifieke certificering mag eisen als een andere, gelijkwaardige vorm van controle dezelfde waarborgen biedt. Door uitsluitend een ISAE 3402 of SOC 1 Type II rapport te eisen, sluit u mogelijk andere partijen uit die op basis van alternatieven voldoen aan de BIO en GIBIT. 4) In eerdere aanbestedingen heeft de IBD aangegeven dat het stellen van een specifiek kwaliteitskeurmerk als harde eis in strijd kan zijn met de BIO en dat inschrijvers de mogelijkheid moeten hebben om een GAP-analyse en Statement of Compliance te overleggen om aan te tonen hoe zij aan de eisen voldoen. Onze vraag: Bent u bereid om de eis van een ISAE 3402 of SOC 1 Type II rapport te heroverwegen en te erkennen dat een TPM gecombineerd met een ISO 27001-certificering met een passende scope, in samenhang met een GAP-analyse en Statement of Compliance ten opzichte van de BIO-eisen, voldoende invulling geeft aan de gewenste beveiligingsmaatregelen? Zo nee, kunt u onderbouwen waarom deze eis proportioneel is in het licht van de uitgangspunten van de GIBIT, BIO, de proportionaliteitseisen uit de Aanbestedingswet, en de analyse in Advies 689 van de Commissie van Aanbestedingsexperts?"	Niet akkoord. Daarnaast wil de gemeente een nuance aanbrengen aan het genoemde in NVI 1. Het is belangrijk te vermelden dat de eis interpretabel is. De eis richt zich op onafhankelijk bewijs, door een partij die daar aantoonbaar toe in staat is, dat de informatieveiligheid voldoet aan de gestelde eisen van de opdrachtgever. ISAE 3402 en SOC 1 type II worden genoemd als voorbeelden, maar zijn niet exclusief vereist. Andere verklaringen kunnen ook worden geaccepteerd, zolang ze aantonen dat aan de eisen wordt voldaan ter beoordeling van de gemeente.
2	Nv1, vraag 98, vraag 119 PvE, Eis 221	Gezien het specifieke gebruik en doel van de ISAE3402-verklaring binnen uw bedrijfsvoering lijkt het ons billijk dat u de jaarlijks terugkerende kosten draagt voor het onderzoek en het opstellen van de verklaring / rapportage. Kunt u dit bevestigen?	Niet akkoord. De prijs dient onderdeel te zijn van de inschrijving. Dit kan worden verdisconteerd bij de jaarlijks terugkerende kosten in het prijzenblad.
3	Nv1, vraag 98, vraag 119 PvE, Eis 221	Kunt u bevestigen dat het proces voor het afgeven van de eerste verklaring / rapportage een jaar na de livegang van de applicatie in gang gezet dient te worden?	Niet akkoord. De eerste verklaring wordt ook het eerste jaar, in 2025, verwacht.
4	Nv1, vraag 98, vraag 119	Wij begrijpen uiteraard uw behoefte om uw gemeentelijke verantwoordelijkheid op aantoonbare wijze in te vullen waarbij een jaarlijks uit te voeren onderzoek en ISAE3402-verklaring dit ondersteunen voor de burgerzakenapplicatie. Echter, zoals blijkt uit de in vragenronde 1 gestelde vragen met betrekking tot de ISAE3402-verklaring is deze verklaring niet voorgeschreven van toepassing voor een Burgerzaken-applicatie en zien wij deze eis dan ook zelden tot nooit in een aanbesteding voor een burgerzaken-applicatie. Daar waar de eis wel wordt gesteld, wordt deze op grond van dezelfde argumentatie als in de vragen 98 en 119 gegeven, alsnog niet van toepassing verklaard. Wij vragen uw antwoord op de vragen 98 en 119 om die reden te heroverwegen en de eis alsnog niet toepasselijk te verklaren.	Niet akkoord. Daarnaast wil de gemeente een nuance aanbrengen aan het genoemde in NVI 1. Het is belangrijk te vermelden dat de eis interpretabel is. De eis richt zich op onafhankelijk bewijs, door een partij die daar aantoonbaar toe in staat is, dat de informatieveiligheid voldoet aan de gestelde eisen van de opdrachtgever. ISAE 3402 en SOC 1 type II worden genoemd als voorbeelden, maar zijn niet exclusief vereist. Andere verklaringen kunnen ook worden geaccepteerd, zolang ze aantonen dat aan de eisen wordt voldaan ter beoordeling van de gemeente.
5	Demonstratie	Indien het de kwaliteit van de demonstratie ten goede komt, mag de volgorde waarin de casussen getoond worden vrij ingevuld worden door leverancier?	Dat is akkoord, mits wordt voldaan aan de volledige scope én het beoogd doel van de casussen. Er zal ten alle tijde worden beoordeeld conform beoordelingsmethodiek in paragraaf 5.4.1.
6	Demonstratie	In de offerteaanvraag leest leverancier dat 1 van de 4 hoofddoelstellingen is: "Een applicatie die e-diensten bevordert, waarmee inwoners zaken zoals verhuizingen, aanvragen van documenten en andere registraties zelfstandig online kunnen regelen". Gezien de zwaarte van de wegging op de demonstratie zien wij niet hoe dit punt getoetst gaat worden tijdens de demonstraties. De afgelopen jaren is door leverancier veel geïnvesteerd in de kwaliteit van e-diensten. Hierin zit veel intelligentie ingebouwd die gebruiksgemak bevordert en het toont de integraliteit van de applicatie aan. Voorbeeld hierbij is onze e-dienst voor Vestiging vanuit het Buitenland (OPENinschrijving). Landelijk heeft leverancier een selfservice percentage van 79%, behaald door 175 gemeenten. Zou de opdrachtgever e-diensten willen toevoegen in de demonstratie casussen? Zo niet, hoe gaat opdrachtgever dan toetsen hoe deze doelstelling gehaald wordt?	E-diensten worden niet expliciet getoetst in de aanbesteding. Wij hebben gekozen voor een gestandaardiseerde beoordeling, gericht op de gevraagde criteria, om een objectieve vergelijking tussen leveranciers mogelijk te maken. Daarnaast zie ook vraag 8.
7	Demonstratie	In het antwoord op vraag 114 geeft u aan dat de zeven testers tegelijkertijd handelingen uit moeten kunnen voeren. Is het akkoord dat, vanwege het gebruik van hardware, testers op elkaar moeten kunnen wachten wanneer de hardware in gebruik is? Dit kan in de praktijk namelijk ook voorkomen.	Zie ook vraag 117 in NV1. Hierin worden twee vragen gesteld, maar wordt er niet direct antwoord gegeven op de vraag of er hardware meegenomen moet worden. Dit is wat ons betreft aan de leverancier zelf. Indien dit ten goede komt voor de uitwerking van de casus, dan is dat toegestaan. Indien, zoals gevraagd in vraag 8 (deze vraag), dan verwacht moet worden op de hardware, dan is dat geen probleem. Wel zal de tijd voor de beoordelaars doorlopen.
8	Demonstratie	Mag de leverancier onderdelen aan de casussen toevoegen die initieel niet uitgevraagd zijn om waar mogelijk het proces beter in beeld te brengen?	Dit is akkoord mits daarmee de scope en het beoogd doel van de casus, bijvoorbeeld "het doen van een verhuizing", ten goede komt en de casus op zich niet significant wijzigt. Er zal ten alle tijde worden beoordeeld conform beoordelingsmethodiek in paragraaf 5.4.1.
9	Demonstratie	Mag de leverancier zelf bepalen welke personen in de testcases staan? Hiermee worden persoonsgegevens en andere relevante informatie bedoeld. Daarmee kan de kwaliteit van de procesflow gegarandeerd worden. En weten we zeker dat de testers niet tegen functionele beperkingen aanlopen m.b.t. gegevens uit de testcases.	Dat is akkoord, mits wordt voldaan aan de volledige scope én het beoogd doel van de casussen. Zo zal, als voorbeeld bij de eerste inschrijving, een niet EU-onderdaan ingeschreven moeten worden en geen inschrijving van iemand binnen de EU. Er zal ten alle tijde worden beoordeeld conform beoordelingsmethodiek in paragraaf 5.4.1.
10	Demonstratie	In het antwoord op vraag 110 stelt u dat land van herkomst, nationaliteit en document aangepast moeten worden naar een niet-EU entiteit. Graag bevestiging dat leverancier deze casus zelf verder mag invullen en mag afwijken van de gestelde gegevens als namen, geboorteplaats en land van herkomst.	Dat is akkoord. Zie antwoord vraag 9.
11	Demonstratie	Graag bevestiging of opdrachtgever of leverancier de vereiste documenten die uitgevraagd worden in de casussen beschikbaar moet stellen.	De leverancier zal de vereiste documenten beschikbaar moeten stellen.
12	Demonstratie	Als antwoord op vraag 84 geeft opdrachtgever aan dat zeven personen de casussen zullen doorlopen. Betekent dat ook dat zeven laptops beschikbaar moeten zijn om de casussen op te doorlopen?	De beoordelaars kunnen hun eigen laptop gebruiken, maar de leverancier mag ook laptops beschikbaar stellen indien het nodig is. Geef dit duidelijk aan bij de inschrijving zodat de gemeente hier rekening mee kan houden.
13	Offerteaanvraag – 5.4 Kwaliteit Demoscenario's	Kan de opdrachtgever concreet maken wat buiten de assistentie van testers tijdens de demo valt? En mag alleen geassisteerd worden op verzoek van de testers of is eigen initiatief van leverancier ook toegestaan?	Er mag alleen geassisteerd worden op nadrukkelijk verzoek van de beoordelaar. Hij/zij zal zelf moeten aangeven behoefte te hebben aan ondersteuning ten behoeve van het uitvoeren van de casus.

14	Offerteaanvraag – 5.4 Kwaliteit Demoscenario's	Dank voor de huidige aanpassing van de demonstratie-opzet tot dusver. De huidige opzet is nu dat de leverancier een uur demonstreert/presenteert en de testers een uur testen. Beide uren bevatten alle drie de uitgevraagde casussen met veel inhoudelijke informatie. Hierdoor zien wij het risico dat focus ontbreekt en informatie onvoldoende overkomt bij iemand die de applicatie niet kent en/of geen vakkennis heeft. Om dit te voorkomen stellen wij een nieuwe opzet en indeling van de demonstratie voor. Casus 1: demonstratie leverancier 30 minuten, testen opdrachtgever 30 minuten. Casus 2: demonstratie leverancier 30 minuten, testen opdrachtgever 30 minuten. Casus 3: demonstratie leverancier 30 minuten, testen opdrachtgever 30 minuten. Hiermee creëren we de juiste context en focus per casus en voorkomen we dat testers van opdrachtgever vastlopen in het proces. Bovenstaand voorstel komt ons inziens de kwaliteit van de demonstratie én het doen van de testen ten goede. Gaat u akkoord met deze opzet? Zo niet, wil opdrachtgever dan 30 minuten toevoegen aan de duur van de demonstratie zodat de leverancier de voor opdrachtgever onbekende applicatie kan demonstreren?	Akkoord met de opzet om, zoals voorgesteld, per casus 30 minuten te demonstreren en daarna 30 minuten door de beoordelaars te laten testen.
15	Offerteaanvraag – 5.4 Kwaliteit Demoscenario's	Is het voor leverancier mogelijk om voorafgaand aan de demonstratie 30 minuten eerder, dus buiten de gestelde 2 uur, de ruimte te kunnen betreden om alle apparatuur voor de demonstraties te kunnen installeren?	Dat is akkoord. Daarnaast wordt de tijd opgerekt naar 3 uur (zie antwoord 15), maar zal er ten alle tijde 30 minuten voorbereidingstijd mogelijk zijn.
16	Programma van Eisen - 219 - BIO en Normen	Hier valt een stuk tekst weg dat relevant is voor het beoordelen van het stellen van een vervolgvraag. De BIO 2 en de implementatie van NIS2 naar de CBW is nog volop in ontwikkeling. Daarmee kunnen wij ook nog geen inschatting maken van de kosten die dit teweegbrengt, en we dit ook nog niet kunnen meenemen in de prijs. Kleine regels rond security kunnen financieel grote impact hebben. Bijvoorbeeld in de BIO 2.0 dat elke internetfacing applicatie bij elke release opnieuw gepentest moet worden. Met continuous delivery en een aantal major-releases per jaar zijn dit kostbare processen om in te richten. Is het voor opdrachtgever acceptabel dat er bij buitenproportionele wijzigingen in de normenkaders in overleg getreden wordt over de wijze waarop de kosten verrekend worden?	In NV1 staat geschreven dat de opdrachtgever proportionaliteit borgt door een gezamenlijke risicoanalyse en impactbeoordeling uit te voeren, waarin de noodzakelijkheid en haalbaarheid van aanvullende eisen worden vastgesteld. Dit proces vindt plaats conform BIO-maatregel 15.1.1.1. Dit antwoord geeft al richtlijnen en handvatten om, bij buitenproportionele wijzigingen in de normenkaders, in overleg te gaan en daarin mogelijk ook te spreken over de verrekening van de kosten.
17	Offerteaanvraag – 5.1 Gunningscriterium	U gaat niet mee in het voorstel om een bodemprijs op te nemen. In de praktijk wordt dit vaak opgenomen om abnormaal lage inschrijvingen te voorkomen. Kunt u dan aangeven welke criteria u hanteert om te controleren wat een 'abnormaal lage inschrijving' is?	De gemeente Meppel heeft voorafgaand aan de aanbesteding een raming opgesteld. Als de inschrijvingen buitenproportioneel afwijken, zullen er verduidelijkingsvragen worden gesteld aan de bewuste inschrijver.
18	Offerteaanvraag - 5.5 gunningscriteria "Plan van Aanpak" en "Programma van Opties"	Bij de puntentoekenning van de demonstratie wordt een doorberekening gemaakt van 150 naar 500 punten. Bij de score van het Programma van opties en het Plan van aanpak kan leverancier o.i. 50 punten behalen gelet op de puntenschaal en de vijf beoordelingscriteria. Kunt u bevestigen dat deze 50 punten worden omgerekend naar 150 maximaal te behalen punten in dezelfde lijn van de berekening bij de demonstratie of specificeren hoe u dit bedoeld heeft?	Zie hoofdstuk 5.5.1. De totaalscore per gunningscriterium is de som van de scores voor alle beoordelingsaspecten. Voor beide gunningscriteria geldt een maximale score van 150 punten. De gunningscriteria "Plan van Aanpak" en "Programma van Opties" worden beoordeeld volgens bovenstaande methodiek. Bij een score van 10 zijn er 150 punten te behalen per gunningscriterium.
19	GIBIT 2023 art. 16.5 iii - iv	Helaas is het onderste stuk van u antwoord weggevallen, waardoor onduidelijk is wat uw antwoord met betrekking tot de vrijwaring voor boetes is. Kunt u uw antwoord vanaf "Art 16 betreft een vrijwaring voor boetes van (...)" herhalen?	Hierbij het vervolg van het antwoord: Art 16 betreft een vrijwaring voor boetes van overheidswege die worden opgelegd vanwege gedragingen of nalaten te wijten aan de opdrachtnemer. Gezien de aard van dit type boete (een overheidstoezichtshouder die een boete oplegt en waarbij het verwijtbaar is aan opdrachtnemer) is het niet akkoord om deze bepaling te laten vallen. Immers, Opdrachtgever heeft geen invloed op betreffende boete, daar het verwijtbaar is aan Leverancier.

20	GIBIT 2023 art. 13	Artikel 13.1: nadere specificering van "passende alternatieven" en de procedure bij nieuwe wetgeving: In het geval dat er nieuwe wetgeving met betrekking tot Algoritmische toepassingen van kracht wordt na het sluiten van de overeenkomst, bestaat er een kans dat de algoritmische toepassing op de schop gegooid moet worden om aan de regelgeving te voldoen. Dit kan mogelijk een duur en complex proces zijn, waarbij het beste alternatief eventueel een andere toepassing of het weglaten van de algoritmische toepassing is (met vervangend alternatief). Leverancier zal in dit geval een voorstel (inclusief eventuele meerkosten) voorleggen aan de gemeente. Het is vervolgens aan de gemeente om hier wel of niet mee akkoord te gaan. Dit zal dus in overleg gebeuren. Artikel 13.4: definitie "noodzakelijkheid" en "derden": de voorgestelde bepaling maakt dat de gemeente haar informatie mag delen met elke derde voor zover een wettelijke verplichting haar oplegt om de informatie te delen met deze betreffende derde. De definitie van noodzakelijkheid is: op basis van een uit de wet volgende verplichting. De definitie van derden is: elke uit de betreffende wettelijke bepaling volgende partij. Artikel 20.7: verduidelijking "gelijkwaardig" en hoe dit wordt beoordeeld: zoals volgt uit de toelichting op de GIBIT 2023 wordt hiermee geborgd dat de gemeente gebruik kan blijven maken van de voor haar relevante functionaliteit bij claims van derden dat de gebruikte ICT Prestatie inbreuk maakt op hun rechten. Het is uiteindelijk aan de gemeente en leverancier samen om te beoordelen of dit ook het geval is in de praktijk. Daarnaast staat voor leverancier ook de ontbindingsmogelijkheid zoals volgt uit artikel 20.8 open.	Op basis van de voorgestelde aanpassingen van artikel 13 in NV1, alsmede de toelichting in NV12, kunnen wij akkoord gaan met het voorstel.
21	Bijlage G - Programma van eisen, #209	Kunt u voor de zekerheid bevestigen dat u met 'en dat de databeveiliging op alle niveaus geborgd is' bedoelt dat met de databeveiliging is geborgd dat de gegevens niet vermengd worden?	Dat is correct.
22	Bijlage G - Programma van eisen, #143	Leverancier kan er niet voor instaan dat derden aan bepaalde verplichtingen voldoen. Zij heeft hier immers alleen controle over middels contractuele afspraken. Wel kan zij aan derden de contractuele verplichtingen opleggen betreffende gedrag, vertrouwelijkheid en bescherming van gegevens. Kunt u bevestigen dat dit voldoende is?	Dat is akkoord.
23	Bijlage G - Programma van eisen, Algemeen	In de toelichting bij diverse eisen worden garantieverplichtingen of waarborgen genoemd, terwijl deze niet expliciet in de eisen zelf zijn opgenomen. Kunt u bevestigen dat deze garantieverplichtingen en waarborgen bedoeld zijn als verduidelijking van de eisen, en dat termen zoals 'garandeert' en 'waarborgt' in dit kader gebruikt worden als alternatief voor 'zorgt voor'? En deze garanties en waarborgen niet bedoeld zijn als verzwaarde verplichtingen?	Dat is correct.
24	Offerteaanvraag - 2.2 Planning aanbestedingsprocedure	Hoewel inschrijver hoopt u de maximale looptijd van dienst te mogen zijn. Kunnen zich (onverwachte) scenario's voordoen waardoor ook inschrijver de overeenkomst moet kunnen opzeggen. Kunt u ermee akkoord gaan dat ook inschrijver de overeenkomst kan opzeggen, na de initiële looptijd, met inachtneming van een opzegtermijn van 12 maanden?	Niet akkoord. Gezien het een kritische applicatie voor de gemeente Meppel betreft kunnen wij hier niet in mee gaan.
25	Bijlage G - Programma van eisen, #207	Momenteel hebben wij nog geen koppeling met Canon Uniflow online en we kennen deze wens nog niet vanuit andere gemeenten. Hierdoor kunnen we de specificaties niet duiden. Is het voor u acceptabel dat wij de aansturing doen op basis van IPPS en dat wij anders onderzoeken op welke wijze wij deze koppeling kunnen ondersteunen?	Dat is acceptabel.
26	Offerteaanvraag – 5.4 Kwaliteit Demoscenario's	De scenario's zijn logischerwijs grotendeels beschreven op basis van de bij u bekende burgerzakenapplicatie. Daardoor is het mogelijk verwarrend wat de stappen zijn om het bedoelde scenario te doorlopen in een specifieke burgerzakenapplicatie. Is het daarom akkoord dat we een stappenplan uitdelen bij de start van de beoordelingsfase?	Indien in de applicatie stappen genomen moeten worden om het doel van de casus te borgen, dan mogen er geringe aanpassingen gedaan worden. Zie ook antwoord 7 en 9.
27	Bijlage G - Programma van Eisen – Eis 221	Wij delen uw opvatting dat de ISAE3402-verklaring veel verder gaat dan de TPM-verklaring en de ISO27001-certificering. Voor ons is leidend dat de scope van de ISAE3402-verklaring zekerheid geeft over het bestaan (type 1) en de werking (type 2) van onze interne beheerprocessen rond informatiebeveiliging en privacy. Processen die naar onze mening zeer relevant zijn voor een burgerzakenapplicatie, en bovendien qua verantwoording goed aansluiten bij de vanuit wetgeving (AVG, CBW) strenger wordende eisen rond informatiebeveiliging en privacy. Voor de SOC1 vraagt u expliciet om type 2 (aantonen van effectieve werking). Voor de ISAE benoemt u dit niet expliciet. Met het oog op de CBW kunnen we ons voorstellen dat u ook voor de ISAE3402-verklaring type 2 op prijs stelt. Kunt u aangeven of u voor ISAE3402 ook type 2 vereist (aantonen effectieve werking), of dat type 1 (aantonen bestaan) volstaat?	Dat is correct. ISAE3402 type 2 of gelijkwaardig/vergelijkbaar volstaat. Zie ook antwoord vraag 1 en 4.
	Mededeling aanbestedende dienst	Aanpassing datum demonstratie en uitwerking casus	In verband met interne complicaties moeten de data van de demonstraties worden herzien. Hieronder worden de nieuwe data kenbaar gemaakt. Maandag 10 februari ochtend 09:00 – 12:00 uur* Maandag 17 februari gehele dag 09:00 – 12:00 en 13:00 – 16:00 uur We gaan ervan uit dat de sessie 3 uur duurt en er een mogelijkheid is om 30 minuten ervoor op te bouwen. Maandag 10 februari zal alleen van toepassing zijn bij 3 inschrijvers. Indien er 2 of minder inschrijvers zijn zal maandag 17 februari van toepassing zijn.