Ref. Nr.	Onderwerp	Vraag	Antwoord
37	E4	Opdrachtnemer is als S2P-platform voor de publieke sector niet formeel gecertificeerd tegen de Gemma basisarchitectuur. De beveiligings- en governanceprincipes die ten grondslag liggen aan Gemma, waaronder informatiebeveiliging, gegevensverwerking binnen de EU, toegangsbeheer en bedrijfscontinuïteit, zijn bij ISPnext geborgd via onze ISO 27001-certificering en ISAE 3402 Type II-auditverklaring. Beide certificeringen zijn jaarlijks onafhankelijk geaudit en valideren de opzet en werking van onze beveiligings- en dienstverlenercontroles. Kunt u bevestigen dat we hiermee aan de eis voldoen?	Ja, dit is akkoord De door inschrijver genoemde certificeringen, te weten ISO/IEC 27001 en ISAE 3402 Type II, worden door de aanbestedende dienst beschouwd als een passend en gelijkwaardig middel om invulling te geven aan de onderliggende principes van GEMMA. Hiermee wordt voldaan aan de gestelde eis.
38	E12	Opdrachtgever kan een extra omgeving beschikbaar stellen tbv het uitvoeren van beheertaken of het verzorgen van opleidingen. Dit is geen gesynchroniseerde omgeving. Volstaat deze werkwijze?	Ja, dit volstaat, mits de aangeboden omgeving aantoonbaar functioneert als acceptatieomgeving en geschikt is voor het uitvoeren van beheertaken en het verzorgen van opleidingen gedurende de project- en gebruiksfase.
39	E14	Opdrachtgever kan een extra omgeving beschikbaar stellen tbv het uitvoeren van beheertaken of het verzorgen van opleidingen. Dit is geen gesynchroniseerde omgeving. Volstaat deze werkwijze?	Nee, dit volstaat niet. De eis ziet expliciet op het periodiek (semi)geautomatiseerd synchroniseren van de acceptatie- en productieomgeving. Een afzonderlijke, niet-gesynchroniseerde omgeving voor beheer- of opleidingsdoeleinden geeft hier geen invulling aan en wordt derhalve niet als gelijkwaardig beschouwd. Het gaat hierbij om periodieke synchronisatie, niet om continue of real-time synchronisatie, waardoor er geen vereiste is dat de omgevingen constant identiek zijn.
40	E32	Opdrachtnemer heeft een API koppelvlak en kan bepaalde essentiële data klaar zetten zodat een ander systeem deze data op kan halen. Het API koppelvlak van Opdrachtnemer beschrijft de mogelijkheden er zijn voor het ontsluiten van gegevens. In deze eis wordt gesteld dat de Gemeente de mogelijkheid heeft om aan te geven welke gegevens er ontsloten moeten kunnen worden. Deze eis is in strijd met E27 (waarin duidelijk wordt om welke gegevens het gaat). Op basis van E27 kunnen Opdrachtnemers aangeven of het haalbaar is of niet. E32 is niet concreet genoeg waardoor Opdrachtnemers niet aan kunnen geven of dit mogelijk is. Wilt u om deze reden deze eis laten vallen?	E27 en E32 zijn niet tegenstrijdig. E27 specificeert de minimale gegevensuitwisseling met het financiële systeem, terwijl E32 de gemeente de mogelijkheid biedt om aanvullend gegevens te ontsluiten. E32 wordt behouden om flexibiliteit voor toekomstige koppelingen te waarborgen.
41	E45	Opdrachtnemer levert een SaaS oplossing. Omdat cloud leveranciers in sprints werken waarbij standaard software wordt uitgerold voor alle klanten is deze eis, in onze ogen, niet van toepassing op het type dienstverlening van een cloud leverancier. Bent u bereid om deze eis te laten vallen?	Nee, de aanbestedende dienst is niet bereid deze eis te laten vervallen. De eis heeft betrekking op het tijdig verwerken van wijzigingen in relevante standaarden waarop het systeem moet aansluiten. Deze verplichting is onafhankelijk van het gehanteerde leveringsmodel (zoals SaaS) en blijft derhalve onverkort van toepassing.
42	E56	We streven bij het bouwen van nieuwe functionaliteit naar niveau A + AA. Echter kunnen we dit niet voor alle onderdelen garanderen. Kunt u bevestigen dat deze werkwijze volstaat?	Ja, dit is akkoord. De user interface voor externe dienstverlening dient te voldoen aan de Web Content Accessibility Guidelines (WCAG) niveau A en AA. Het door inschrijver beschreven uitgangspunt wordt als passend beschouwd.
43	E67	Dez eis ligt in het verlengde van de vragen over E12 en E14. Opdrachtnemer kan een extra omgeving opleveren maar deze is niet gesynchroniseerd. Volstaat deze werkwijze?	Zie antwoord vraag 39
44	E75	Wordt hiermee bedoelt dat bepaalde velden niet meer te wijzigen zijn voor bepaalde rollen nadat een contract een bepaalde status heeft gekregen?	Ja, dat klopt. De eis ziet erop dat bepaalde informatieobjecten, zoals een contract, definitief gemaakt kunnen worden en dat velden daarna niet meer wijzigbaar zijn voor de betreffende rollen, met een waarschuwing dat wijzigen niet mogelijk is.
45	E78	Onder NDA is het mogelijk om onze ISAE verklaring te ontvangen in het eerste kwartaal van het nieuwe jaar. Voldoet deze werkwijze voor Opdrachtgever?	Ja, deze werkwijze volstaat. De eis verlangt dat jaarlijks en op eerste verzoek een verklaring van een onafhankelijke derde kan worden getoond waaruit blijkt dat de informatiebeveiliging van de organisatie voldoet aan de eisen van de opdrachtgever, ten behoeve van ENSIA- en WPG-audits op basis van het NOREA-normenkader.
46	E80	Vooralsnog werken we met wildcards waar we overwegen om hier vanaf te stappen. Volgens ons ISAE 3402 security framework hebben we beveiligingsmaatregelen getroffen om de veiligheid te garanderen. Voldoet deze werkwijze?	Nee, de gemeente houdt vast aan de eis dat wildcard-certificaten niet zijn toegestaan. Voor systeemkoppelingen dienen SAN-certificaten binnen een omgeving of PKI-certificaten te worden gebruikt, conform de aanbestedingseisen.
47	E83	Alle mutaties binnen contracten en leveranciers worden vastgelegd binnen een audittrail, inclusief wie (gebruiker of systeem), wat (veld en oude/nieuwe waarde), wanneer (datum/tijd) en hoe. Kunt u bevestigen dat we hiermee aan de eis voldoen?	Ja dit volstaat
48	E85	Kunt u toelichten wat het loggingbeleid is van de gemeente?	De verwijzing doelt op het strategisch informatieveiligheidsbeleid van de gemeente (openbaar beschikbaar). Betreft logging zijn de eisen als in het PvE opgenomen de logische doorvertaling hiervan.
49	PvE 4.1.6	Bij het verwijderen van een leverancier wordt geen actieve controle uitgevoerd op onderliggende contracten. Deze contracten blijven zichtbaar in het systeem, waarbij duidelijk is dat de gekoppelde leverancier is verwijderd. Daarnaast is in het leverancierspro fiel altijd inzichtelijk welke contracten aan een leverancier zijn gekoppeld. Het is daarom onwaarschijnlijk dat een gebruiker met rechten om een leverancier te verwijderen, dit doet zonder de gevolgen voor de onderliggende contracten mee te wegen. Bent u bereid deze eis te laten vervallen, mede gelet op het feit dat: het recht om een leverancier te verwijderen beperkt kan worden; In het leverancierspro fiel altijd inzichtelijk is welke contracten aan een leverancier zijn gekoppeld; op contractniveau duidelijk is of de leverancier is verwijderd; er overzichten beschikbaar zijn van contracten waarbij de leverancier is verwijderd zodat deze contracten indien gewenst geschorst, gearchiveerd of verwijderd kunnen worden.	Opdrachtgever is van mening dat de beschreven werkwijze/functionaliteit volstaat.