

Nr in PVE ICO-wizard	Vraag	Antwoord
932	De gevraagde SOC2-certificering betreft van oorsprong een Amerikaans normenkader. Om optimaal aan te sluiten bij de vigerende Nederlandse en Europese standaarden voor informatiebeveiliging, verzoeken wij u te bevestigen of de Aanbestedende Dienst de volgende combinatie van onafhankelijk getoetste en geaccrediteerde waarborgen accepteert als een volwaardig en gelijkwaardig alternatief voor de SOC2-eis: 1. Geaccrediteerde Procesborging: Een geldig ISO 27001 certificaat voor ons Information Security Management System (ISMS), afgegeven door een RvA-geaccrediteerde certificatie-instelling. 2. Onafhankelijke Technische Verificatie: Periodieke penetratietesten op de applicatie en infrastructuur, uitgevoerd door een CCV-geaccrediteerde cybersecuritypartij conform de hoogste Nederlandse standaard. 3. Aantoonbaarheid (Assurance): Een actuele uitwerking en mapping op de vereiste CSA Cloud Control Matrix (CCM), gecombineerd met een 'right to audit'. Biedt deze combinatie van procesmatige en technische accreditaties voor de Aanbestedende Dienst de gewenste, gelijkwaardige mate van assurance voor deze opdracht?	Een SOC2-rapportage is enkel nodig wanneer meer dan gewone persoonsgegevens worden verwerkt. Daar is in dit geval geen sprake van en daarom volstaat een recente ISO27001-certificering.
932	De eis stelt dat de CSP gedurende de gehele contractperiode over een SOC2 Type 2 verklaring moet beschikken voor de volledige scope van de werkzaamheden. De Aanbestedende Dienst geeft echter aan dat een aanzienlijk deel van de softwarecomponenten en specifieke inrichting pas na ingang van de overeenkomst (1 juli) wordt gerealiseerd. Een Type 2 Assuranceverklaring toetst de effectieve werking van beheersmaatregelen over een reeds verstreken periode (doorgaans de voorafgaande 6 tot 12 maanden). Kan de Aanbestedende Dienst bevestigen dat het feitelijk onmogelijk is om op 1 juli een Type 2 verklaring te overleggen die de 'volledige scope' van de nog te realiseren werkzaamheden afdekt? Gezien het bovenstaande: is de Aanbestedende Dienst, om de innovatieve realisatiefase niet te blokkeren, bereid de eis te herformuleren naar een ingroepiad? Hierbij zou de Assurance-verplichting (Type 2) pas van kracht worden nadat de realisatiefase is afgerond en er een representatieve operationele periode heeft plaatsgevonden, waarbij de huidige ISO 27001/NEN 7510 certificeringen van Inschrijver tot die tijd als gelijkwaardig worden geaccepteerd.	Het volstaat om de clouddienstverlener de ISO 27001/NEN 7510 certificaten te laten aanleveren.

932	In het PvE constateren wij een tegenstrijdigheid die wij graag aan u voorleggen. Enerzijds stelt u (onder andere via de NBIV/BBN2 kaders en eis 860) zeer strikte eisen aan digitale soevereiniteit en de uitsluiting van buitenlandse statelijke invloeden (zoals de US CLOUD Act). Dit sluit het gebruik van Amerikaanse Public Cloud-aanbieders in de praktijk uit. Anderzijds eist u een SOC2 Type 2 verklaring. Dit is een Amerikaanse standaard die in Nederland vrijwel uitsluitend door diezelfde uitgesloten Amerikaanse Public Cloud-partijen wordt gehanteerd. Onze inschatting is dat geen enkele gegadigde aan deze paradoxale combinatie kan voldoen. Door onverkort aan de SOC2-eis vast te houden, sluit u de veiligste lokaal verankerde oplossingen uit en bestaat de kans dat er geen inschrijvingen volgen. Om een succesvolle aanbesteding met volledig soevereine oplossingen mogelijk te maken, verzoeken wij u te bevestigen of u onderstaande combinatie van onafhankelijk getoetste waarborgen accepteert als een volwaardig en gelijkwaardig alternatief: - Geaccrediteerde Procesborging: Een geldig ISO 27001 certificaat (RvA-geaccrediteerd). - Onafhankelijke Technische Verificatie: Periodieke penetratietesten door een CCV-geaccrediteerde partij conform de hoogste Nederlandse standaard. - Aantoonbaarheid: Een actuele mapping op de vereiste CSA Cloud Control Matrix (CCM), gecombineerd met een 'right to audit'. Graag vernemen wij of u hiermee instemt.	Allereerst: hier is zeker geen sprake van een "paradoxale combinatie". Een SOC2-rapport (type 2) is ook in Europa een geaccrediteerde auditvorm om zo bij een organisatie te onderzoeken of deze voldoet aan beveiligingsstandaarden. Oorsprong is inderdaad Amerikaanse standaarden, maar dat is de ISO ook. Een SOC2-rapportage/audit is een gedetailleerd onderzoek en gaat op technisch vlak nog veel dieper in vergelijking met een ISO27001-audit. Het kijkt naar wat op schrift staat (beleid) en of deze ook technisch kan worden geborgd en operationeel werkt. Terwijl de ISO27001 zich vooral bezig houdt met procesbeveiliging, toont een SOC2-rapport aan dat de controls ook in de praktijk werken. BEIDE zijn raamwerken voor informatiebeveiliging die aantonen dat een organisatie veilig met data omgaan. Het voorgestelde alternatief wordt als gelijkwaardig beschouwd indien: - Clouddienst voldoet aan archiefwet en WOO. - Clouddienst is compliant aan de AVG - Clouddienst moet garanderen dat OCW-klantomgeving is gescheiden van andere klantomgevingen. - Serverhardening dient te worden toegepast (eventueel via encryptie) Een SOC2-rapportage is niet nodig mits de clouddienstverlener de technische plannen en getroffen beveiligingsmaatregelen kan aantonen, welke conform het cloudbeleid zijn (Hier te vinden: https://rijksportaal.overheid-i.nl/organisaties/ocw/artikelen/organisatie/directies/sg/kennis/beleidshuis/ai-cloud.html)
198	Eis 198: U geeft hier aan: “Broncode ontwikkeld ten behoeve van de Bijzondere Opdracht wordt nooit opgeslagen door middel van een Cloudoplossing.” Kunt u toelichten wat u bedoelt met ‘Bijzondere Opdracht’? Onze organisatie werkt met cloudgebaseerde DevOps omgevingen (zoals Azure DevOps of GitHub Enterprise), waarbij de broncode logisch en technisch is afgeschermd binnen een EU tenant. Kunt u bevestigen of dit is toegestaan voor de Bijzondere Opdracht?	De voorwaarde dat er geen sprake is van een bijzondere opdracht, een bijzondere Opdracht in het teken van de ABRO (Algemene Beveiligingseisen voor Rijksoverheidsopdrachten 2026) is een inkoopopdracht van de Rijksoverheid waarbij toegang tot of verwerking van gevoelige informatie, systemen of locaties noodzakelijk is, wat risico's met zich meebrengt voor de nationale veiligheid. Het risico van een bijzondere opdracht wordt als volgt omschreven: De opdracht kan leiden tot schade aan vitale belangen van de staat, bondgenoten of ministeries. Bij deze opdracht hebben we te maken met Lage Te Beschermen Belangen (TBB4).
232	Eis 232 stelt dat acceptatie van systemen plaatsvindt nadat is vastgesteld dat de ABRO 2026 eisen zijn geïmplementeerd. Kan worden verduidelijkt welke vorm van aantoonbaarheid hiervoor door Opdrachtgever als voldoende wordt beschouwd (bijvoorbeeld beleidsdocumenten, procesbeschrijvingen, configuratie evidence of assuranceverklaringen)?	Niet alleen processen maar ook de infrastructuur, systemen, het gebouw zelf, het hele pakket, wordt bij een ISO27001 audit meegenomen. Partij geeft aan dat via een ISO27001-certificaat hun processen geborgd zijn. Geldt dit ook voor de informatiesystemen waarmee wordt gewerkt? Een ISO-certificering suggereert het wel.
248	Eis 248: hier wordt onweerlegbaarheid genoemd voor aangewezen transacties. Kan worden bevestigd of binnen het kader van het Monitoringsonderzoek MDT sprake is van transacties waarvoor formele onweerlegbaarheid vereist is?	Binnen het kader van het monitoringsonderzoek is sprake van transacties waarvoor formele onweerlegbaarheid is vereist
algemeen	Kunt u bevestigen dat de infrastructuur en alle hosting geleverd moeten worden door opdrachtnemer, en deze verantwoordelijkheid dus niet bij opdrachtgever ligt?	De technische infrastructuur en alle hosting dient geleverd te worden door opdrachtnemer; deze verantwoordelijkheid ligt niet bij de opdrachtgever.