

Algemene informatie

Aanbesteding: Projectbeheersing systeem (PBS) en ERP#integraties

Aanbestedende Dienst: Provincie Noord-Holland

Referentie: -

Toelichting:

Ter verduidelijking van de eis voor aanmelding met betrekking tot het voldoen aan ISO 27001 is de bijgevoegde vraag en beantwoording gepubliceerd. De termijn voor het stellen van vragen ten behoeve van de NVI blijft ongewijzigd en zal op 14 augustus 2026 sluiten.

Vraag en antwoord

Ref.nr.

1

Onderwerp:

ISO/IEC 27001 of vergelijkbaar

Vraag:

In paragraaf 4.5.1.1 stelt u een geldige ISAE 3402 type II-verklaring als geschiktheidseis, met uitsluiting als sanctie. ISAE 3402 richt zich op beheersmaatregelen die relevant zijn voor de financiële verslaggeving van gebruikersorganisaties, terwijl de beheersingsrisico's bij een SaaS-oplossing primair liggen bij informatiebeveiliging, beschikbaarheid en de verwerking van persoonsgegevens. Voor die risico's is de ISO/IEC 27001-familie de gangbare en objectief toetsbare norm. Bevestigt u dat een geldig ISO/IEC 27001-certificaat, inclusief Verklaring van Toepasselijkheid en aantoonbare toepassing van de beheersmaatregelen uit ISO/IEC 27002, geldt als het in deze paragraaf bedoelde gelijkwaardige niveau van interne beheersing dat door een onafhankelijke auditor is bevestigd? Indien dat niet het geval is, verzoeken wij u toetsbaar aan te geven welke bewijsmiddelen u wel aanvaard, zodat gegadigden vooraf kunnen vaststellen of zij aan deze eis voldoen.

Antwoord:

ISO/IEC 27001 of vergelijkbaar

De aanbestedende dienst stelt vanuit Cybersecurity als eis dat inschrijvers beschikken over een ISO /IEC 27001-certificaat met bijbehorende Verklaring van Toepasselijkheid, of een daarmee vergelijkbaar bewijsmiddel, zoals een ISAE 3402 type II-verklaring. Het doel van deze eis is dat inschrijvers aantonen dat hun informatiebeveiliging en interne beheersing aantoonbaar en op een passend niveau zijn ingericht.

Vergelijkbaar en toetsbaar

De aanbestedende dienst handhaaft de geschiktheidseis zoals opgenomen in paragraaf 4.5.1.1. Deze eis is gesteld om te waarborgen dat de inschrijver beschikt over een aantoonbaar en structureel geborgd niveau van interne beheersing.

De aanbestedende dienst onderkent dat bij SaaS-dienstverlening de nadruk ligt op informatiebeveiliging, beschikbaarheid en bescherming van persoonsgegevens. Om die reden staat de aanbestedende dienst, conform het gelijkwaardigheidsbeginsel, toe dat inschrijvers andere bewijsmiddelen overleggen die een gelijkwaardig niveau van beheersing aantonen. Een geldig ISO/IEC 27001-certificaat, inclusief Verklaring van Toepasselijkheid (Statement of Applicability), wordt door de aanbestedende dienst in beginsel als een passend bewijsmiddel beschouwd, mits de scope van het certificaat de aangeboden dienstverlening dekt en het certificaat is afgegeven door een geaccrediteerde instelling.

Daarnaast kunnen ook andere, door een onafhankelijke derde getoetste assurance-rapportages (zoals SOC 2 Type II of vergelijkbaar) of een combinatie van bewijsmiddelen worden overgelegd, voor zover deze gezamenlijk een aantoonbaar en vergelijkbaar niveau van interne beheersing

onderbouwen.

De aanbestedende dienst beoordeelt de gelijkwaardigheid integraal en risicogericht, waarbij onder meer wordt gekeken naar:

- De reikwijdte (scope) van de toetsing in relatie tot de aangeboden dienstverlening;
- De mate waarin relevante beheersdoelstellingen (waaronder informatiebeveiliging, beschikbaarheid, continuïteit en privacy) zijn afgedekt;
- De onafhankelijkheid en kwaliteit van de toetsende partij;
- De actualiteit en bestendigheid van de aangetoonde beheersmaatregelen.

Met deze formulering beoogt de aanbestedende dienst enerzijds voldoende ruimte te bieden aan gangbare marktstandaarden en anderzijds te borgen dat het vereiste niveau van aantoonbare beheersing objectief toetsbaar blijft.

Inschrijvers wordt geadviseerd om in hun inschrijving expliciet te motiveren op welke wijze met de overgelegde bewijsmiddelen aan deze eis wordt voldaan.

Fase:

Aanmeldfase

Inschrijfronde:

-

Vragenronde:

Vragenronde 1

Beantwoord op:

29 jul 2026

Percelen:

P1 Projectbeheersing systeem (PBS) en ERP#integraties