



Bijlage A – Programma van Eisen

Rijksinkoop samenwerking

Bezoekadres

Rijkskantoor Beatrixpark
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 20011
2500 EA Den Haag

Programma van Eisen

Kenmerk	201865002.284.001
Versie	1.0

Inhoudsopgave

Programma van Eisen	1
1. Toepasselijkheid en karakter van de eisen	3
1.1. Karakter van de eisen	3
1.2. Knock-out eisen	3
1.3. Relatie met Nota van Inlichtingen	3
1.4. Naleving gedurende de looptijd	3
Uitgangspunten	4
1. Algemene eisen aan de opdracht	4
2. Security, Compliance en Digitale Soevereiniteit eisen	5
3. Service Management eisen	7
4. Governance en Samenwerking eisen	9
5. Hosting- en Beheer eisen	10
6. Architectuur eisen	12
7. Applicaties eisen	13
8. Integraties eisen	15
9. Archivering eisen	16
10. Back-up en herstel eisen	16
11. Migratie eisen	17
12. Innovatie eisen	17
13. SIEM/SOC (Optioneel)	18
14. Maatschappelijk Verantwoord Opdrachtgeven en Inkopen (MVOI)	19
15. Gevolgen van niet naleving	21

1. Toepasselijkheid en karakter van de eisen

1.1. Karakter van de eisen

Dit PvE bevat de eisen die van toepassing zijn op de Opdracht.

1.2. Knock-out eisen

Knock-out eisen dienen bij definitieve inschrijving volledig en onvoorwaardelijk te worden geaccepteerd. Indien niet aan deze eisen wordt voldaan, wordt de inschrijving ongeldig verklaard en terzijde gelegd.

1.3. Relatie met Nota van Inlichtingen

De Nota van Inlichtingen (NvI) en het Programma van Eisen (PvE) vormen gezamenlijk de aanbestedingsstukken.

In geval van tegenstrijdigheden tussen het PvE en de Nota van Inlichtingen, prevaleert de meest recente Nota van Inlichtingen.

1.4. Naleving gedurende de looptijd

Inschrijver voldoet uiterlijk op de datum van formele Go-Live (na acceptatie van de migratiefase) aantoonbaar aan alle operationele eisen uit dit Programma van Eisen, en draagt er zorg voor dat gedurende de gehele looptijd van de Overeenkomst blijvend aan deze eisen wordt voldaan. Bij aanvang van de Overeenkomst voldoet inschrijver aan de eisen die randvoorwaardelijk zijn voor de migratiefase

Indien gedurende de looptijd blijkt dat niet (langer) aan één of meer eisen wordt voldaan, is sprake van een toerekenbare tekortkoming in de nakoming van de Overeenkomst, tenzij Inschrijver aantoont dat hem dit niet kan worden toegerekend.

In een dergelijk geval is de Aanbestedende Dienst gerechtigd om, onverminderd overige rechten en rechtsmiddelen:

- de Inschrijver schriftelijk in gebreke te stellen en een redelijke termijn te stellen waarbinnen alsnog volledig aan de eisen wordt voldaan;
- nadere instructies te geven en/of corrigerende en preventieve maatregelen voor te schrijven, alsmede de uitvoering daarvan te (laten) controleren;
- betalingen geheel of gedeeltelijk op te schorten zolang niet aan de eisen wordt voldaan;
- de Overeenkomst geheel of gedeeltelijk te ontbinden, conform de bepalingen in de Overeenkomst.

Uitgangspunten

1. Algemene eisen aan de opdracht

Algemene eisen aan de opdracht				
Eis Algemeen 1.1	Inschrijver levert de dienstverlening vanuit organisaties, personeel en datacenters binnen de Europese Economische Ruimte (EER), vallend onder Europees recht.	KO		
Eis Algemeen 1.2	Aanbestedende Dienst heeft het recht periodiek audits of onderzoeken uit te laten voeren op de dienstverlening. Inschrijver verleent hieraan medewerking.	KO		
Eis Algemeen 1.3	Alle productieomgevingen en dataopslag bevinden zich binnen de Europese Economische Ruimte (EER).	KO		
Eis Algemeen 1.4	Inschrijver treft passende, technische en organisatorische maatregelen om beschikbaarheid, integriteit en continuïteit van de dienstverlening te waarborgen op basis van SLA.	KO		
Eis Algemeen 1.5	Alle data, tenantconfiguraties, domeinnamen en specifiek voor Aanbestedende Dienst ingerichte omgevingen blijven eigendom van Aanbestedende Dienst.	KO		
Eis Algemeen 1.6	Medewerkers met toegang tot systemen of vertrouwelijke informatie beschikken over een geldige VOG voor minimaal het screeningsprofiel 01 – Informatie, 11 en 12	KO		
Eis Algemeen 1.7	Gebruikersinterfaces, beheerportalen en servicedocumentatie zijn beschikbaar in Nederlands of Engels. Bij voorkeur in het Nederlands.	KO		
Eis Algemeen 1.8	Operationele en tactische communicatie vindt plaats in het Nederlands. Sleutelfunctionarissen beheersen Nederlands op professioneel niveau. https://detaalbrigade.nl/taalniveaus	KO		
Eis Algemeen 1.9	Inschrijver werkt mee aan noodzakelijke aanpassingen als gevolg van gewijzigde wet- en regelgeving. Indien substantiële impact ontstaat op dienstverlening of kosten, treden partijen hierover in overleg.	KO		
Eis Algemeen 1.10	Inschrijver verleent bij beëindiging van de overeenkomst medewerking aan overdracht van dienstverlening, data en documentatie conform overeengekomen exit afspraken.	KO		
Eis Algemeen 1.11	Opdrachtgever heeft tijdens de looptijd van het contract het recht om de overeenkomst te ontbinden bij significante wijzigingen in het beleid vanuit de overheid en/of de mogelijkheden die de overheid zelf biedt. Hiervoor zal een opzegtermijn van 1 jaar worden gehanteerd.	KO		
Eis Algemeen 1.12	Inschrijver werkt samen met andere leveranciers en de Opdrachtgever conform de geldende Rijksvoorwaarden (waaronder de ARBIT 2022) en governance afspraken.	KO		
Eis Algemeen 1.13	Inschrijver richt logging, monitoring en beheerprocessen zodanig in dat forensisch onderzoek mogelijk blijft. Deze logging biedt voldoende detailniveau voor incidentanalyse en reconstructie van gebeurtenissen.	KO		
Eis Algemeen 1.14	Inschrijver voldoet aan de Social Return verplichtingen zoals opgenomen in de bijlage van deze aanbesteding.	KO		
Eis algemeen 1.15	Inschrijver stelt Opdrachtgever onverwijld schriftelijk op de hoogte van iedere voorgenomen of gerealiseerde wijziging in de zeggenschap ("Change of Control") over Inschrijver of een bij de uitvoering van de Overeenkomst betrokken groepsmaatschappij. Onder Change of Control wordt verstaan een directe of indirecte wijziging van de feitelijke zeggenschap, waaronder een fusie, overname of overdracht van meerderheid van aandelen of stemrechten. Inschrijver blijft onverminderd verantwoordelijk voor de	KO		

	volledige nakoming van de Overeenkomst. Indien een Change of Control naar het redelijke oordeel van Opdrachtgever risico's oplevert voor de continuïteit, beveiliging of correcte uitvoering van de Overeenkomst, is Opdrachtgever gerechtigd aanvullende waarborgen te verlangen of de Overeenkomst geheel of gedeeltelijk op te zeggen. Inschrijver verstrekt op verzoek alle redelijkerwijs benodigde informatie over de Change of Control.			
--	--	--	--	--

2. Security, Compliance en Digitale Soevereiniteit eisen

Security, Compliance en Digitale Soevereiniteit eisen				
Eisen aan Inschrijver				
Eis Security, Compliance en Digitale Soevereiniteit 2.1	Inschrijver voldoet gedurende de looptijd van de overeenkomst aan de (actuele) Baseline Informatiebeveiliging Overheid.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.2	Inschrijver beschikt gedurende de looptijd van de overeenkomst over een aantoonbaar geïmplementeerd Information Security Management System (ISMS) en is gecertificeerd conform ISO/IEC 27001 of aantoonbaar gelijkwaardige certificering.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.3	Inschrijver maakt de leveranciersketen inzichtelijk en borgt dat kritieke onderleveranciers aantoonbaar voldoen aan passende informatiebeveiligingsnormen en beschikken over een actueel ISO/IEC 27001-certificaat of aantoonbaar gelijkwaardige certificering.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.4	Inschrijver treft technische, organisatorische en contractuele maatregelen ter borging van digitale soevereiniteit van data en dienstverlening binnen de Europese Economische Ruimte (EER).	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.5	Doorgifte van data of toegang tot data buiten de Europese Economische Ruimte (EER) is uitsluitend toegestaan indien wordt voldaan aan de toepasselijke vereisten uit de AVG en voorafgaande schriftelijke toestemming is verkregen van Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.6	Persoonsgegevens worden uitsluitend verwerkt binnen de Europese Economische Ruimte (EER) conform AVG.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.7	Inschrijver verleent medewerking aan Data Protection Impact Assessment (DPIA) en levert tijdig benodigde informatie aan.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.8	Inschrijver voldoet gedurende de looptijd van de overeenkomst aan de AVG.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.9	Inschrijver voert periodiek kwetsbaarheidsscans uit en rapporteert bevindingen, risico's en opvolgmaatregelen. De dienstverlening voldoet aan de onderstaande eisen: • Inschrijver biedt 'Vulnerability scanning' als dienst aan voor de PaaS-omgeving van de aanbestedende dienst; • Deze scans worden periodiek uitgevoerd en omvatten minimaal systemen, netwerken en applicaties, zowel dynamisch als statisch; • Resultaten worden gerapporteerd, inclusief risicobeoordeling en aanbevelingen voor opvolging	KO		

Eis Security, Compliance en Digitale Soevereiniteit 2.10	Inschrijver verstrekt jaarlijks een actuele onafhankelijke assurance-rapportage, zoals SOC2 Type II of ISAE3000 Type II.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.11	Inschrijver beschikt over een formele incidentprocedure voor informatie-beveiligingsincidenten inclusief meld-, escalatie- en rapportageprocessen.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.12	Inschrijver beschikt over een datalekprocedure conform AVG en meldt datalekken tijdig aan Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.13	Inschrijver werkt mee aan noodzakelijke beveiligingsmaatregelen en wijzigingen die voortvloeien uit gewijzigde wet- en regelgeving, rijksbeleid of actuele informatiebeveiligingseisen.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.14	Inschrijver en Aanbestedende Dienst leggen exit afspraken contractueel vast voorafgaand aan ingebruikname van de dienstverlening.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.15	Inschrijver laat minimaal jaarlijks onafhankelijke penetratietesten uitvoeren op de infrastructuur. En rapporteert over opvolging op de gevonden kwetsbaarheden	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.16	Inschrijver verleent medewerking aan zowel audits als penetratietesten uitgevoerd in opdracht van Aanbestedende Dienst.	KO		
Eisen aan het product van Inschrijver				
Eis Security, Compliance en Digitale Soevereiniteit 2.17	De dienstverlening voldoet aan verplichte open standaarden van Forum Standaardisatie en relevante NCSC-richtlijnen. (https://www.forumstandaardisatie.nl/open-standaarden/verplicht) In ieder geval, conform 'Pas toe leg uit' - principe: • Authenticatie-standaarden (OpenID.NLGov en SAML) • DKIM • DMARC • DNSSEC • HTTPS en HSTS • IPv6 • NL GOV Assurance profile for OAuth 2.0 • OpenAPI Specification • REST-API Design Rules • RPKI • Security.txt • SPF • STARTTLS en DANE • TLS • ACME • IPsec • SMTP	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.18	De omgevingen bieden ondersteuning voor 'Single-Sign-On' vanuit omgeving Opdrachtgever. Waar SSO niet mogelijk is wordt minimaal gebruik gemaakt van: • Stepping Stone met 2FA toegang • Gebruik van MFA-methode (soft-token of hard-token) • Bij gebruik van gebruikersnaam en wachtwoord gelden volgende wachtwoord-eisen: ◦ Minimaal 12 tekens	KO		

	- o Geen hergebruik wachtwoorden toestaan - o Na 5 mislukte pogingen een tijdelijke blokkering van het account voor minimaal 30 minuten			
Eis Security, Compliance en Digitale Soevereiniteit 2.19	Data wordt versleuteld opgeslagen en versleuteld verzonden conform actuele beveiligingsstandaarden.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.20	Alle beheer- en gebruikersinterfaces ondersteunen Multi-Factor Authenticatie.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.21	De omgeving is beveiligd tegen DDOS-aanvallen en inschrijver verzorgt risicobeperkende services.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.22	Datacenters voldoen minimaal aan de volgende eisen of gelijkwaardig: • ISO 27001 • ISAE 3402 type 2 • ISO 22301	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.23	De dienstverlening beschikt minimaal over: • centrale logging van beveiligingsgebeurtenissen; • monitoring van infrastructuur, systemen en beveiligingsincidenten; • bewaartermijnen en rapportagemogelijkheden conform afspraken met Opdrachtgever.	KO		
Digitale Soevereiniteit eisen				
Eis Security, Compliance en Digitale Soevereiniteit 2.24	De dienstverlening ondersteunt export van data en configuraties in open en gangbare formaten	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.25	Inschrijver maakt op verzoek inzichtelijk welke onderaannemers en onderleveranciers worden ingezet voor de dienstverlening.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.26	Wijzigingen in kritieke onderaannemers, ketenpartners of de eigendoms- en zeggenschapsstructuur van Inschrijver worden vooraf schriftelijk gemeld aan Opdrachtgever. Opdrachtgever behoudt het recht deze wijzigingen te beoordelen op impact voor informatiebeveiliging en dienstverlening.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.27	Inzet van onderaannemers buiten de Europese Economische Ruimte (EER) is uitsluitend toegestaan na voorafgaande schriftelijke toestemming van Opdrachtgever, mits geen toegang bestaat tot persoonsgegevens, vertrouwelijke gegevens, productieomgevingen of beheerinterfaces van Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.28	Toegang door onderaannemers wordt gelogd en op verzoek inzichtelijk gemaakt voor Opdrachtgever.	KO		
Eis Security, Compliance en Digitale Soevereiniteit 2.29	De dienstverlening ondersteunt overdraagbaarheid naar alternatieve leveranciers door middel van exporteerbare dataformaten, overdraagbare configuraties, documentatie en redelijke exit-ondersteuning bij beëindiging van de overeenkomst.	KO		

3. Service Management eisen

Service Management eisen

Eis Service Management 3.1	Inschrijver en Aanbestedende Dienst stellen gezamenlijk een calamiteitenorganisatie vast inclusief bevoegdheden, escalaties en contactpersonen, aangevuld met een calamiteitenprocedure. Details worden in het DAP uitgewerkt.	KO		
Eis Service Management 3.2	Bij calamiteiten informeert Inschrijver en Aanbestedende Dienst onverwijld conform overeengekomen escalatieprocedures.	KO		
Eis Service Management 3.3	PRIO1-incidenten moeten telefonisch kunnen worden gemeld.	KO		
Eis Service Management 3.4	Inschrijver stelt een servicedesk beschikbaar gedurende overeengekomen servicewindows.	KO		
Eis Service Management 3.5	Meldingen kunnen 24x7 worden ingediend via overeengekomen communicatiekanalen.	KO		
Eis Service Management 3.6	Inschrijver beschrijft maatregelen voor continuïteit en beheersing van afhankelijkheden binnen de dienstverlening.	KO		
Eis Service Management 3.7	Inschrijver monitort capaciteit proactief en adviseert tijdig over benodigde schaalvergroting/-verkleining of optimalisatie.	KO		
Eis Service Management 3.8	Inschrijver onderhoudt actuele configuratie- en beheerdocumentatie inclusief CMDB.	KO		
Eis Service Management 3.9	Inschrijver en Aanbestedende Dienst stellen gezamenlijk een SLA en DAP op voorafgaand aan ingebruikname van de dienstverlening.	KO		
Eis Service Management 3.10	Prioriteiten van meldingen worden vastgesteld conform gezamenlijk overeengekomen classificaties.	KO		
Eis Service Management 3.11	Responstijden en KPI's worden vastgelegd in de SLA. Hiervoor gelden de volgende minimale responstijden: • Prioriteit 1 meldingen: maximaal 15 minuten; • Overige prioriteitsklassen: maximaal 1 uur. De exacte toepasselijkheid van servicewindows per prioriteitsklasse wordt vastgelegd in de SLA. Inschrijver realiseert maandelijks minimaal 90% naleving van de overeengekomen responstijden, gemeten per prioriteitsklasse op basis van geregistreeerde meldingen in het IT Service Management systeem.	KO		
Eis Service Management 3.12	Oplostijden per prioriteitsklasse worden vastgelegd in de SLA. De volgende minimale oplostijden gelden: • Prioriteit 1: binnen 4 uur binnen overeengekomen servicewindow • Prioriteit 2: binnen 8 uur binnen overeengekomen servicewindows. • Prioriteit 3/4/5: binnen 5 werkdagen binnen overeengekomen servicewindows. Inschrijver realiseert maandelijks minimaal 90% naleving van de overeengekomen oplostijden, gemeten per prioriteitsklasse. Metingen vinden plaats op basis van geregistreeerde meldingen in het IT Service Management systeem.	KO		
Eis Service Management 3.13	Inschrijver levert maandelijks rapportages over dienstverlening, incidenten, wijzigingen en afgesproken KPI's.	KO		
Eis Service Management 3.14	Inschrijver rapporteert periodiek over lifecycle-management van relevante hardware- en softwarecomponenten.	KO		

Eis Service Management 3.15	Na ernstige incidenten levert de Inschrijver, binnen 10 werkdagen, een Root Cause Analysis (RCA) inclusief verbetermaatregelen.	KO		
Eis Service Management 3.16	Minimale servicewindows worden vastgelegd in de SLA. Het service window is van maandag t/m vrijdag van 8:00 tot 18:00 uur, uitgezonderd erkende Nederlandse feestdagen. Inschrijver biedt de mogelijkheid om dit service window te verruimen naar maximaal 24 uur x 7, bij verandering van de dienstverlening van Aanbestedende Dienst.	KO		
Eis Service Management 3.17	De IT Service Management tooling van Inschrijver dient koppelbaar te zijn aan de IT Service Management tooling van de Aanbestedende Dienst.	KO		
Eis Service Management 3.18	Geplande onderhoudswerkzaamheden worden uitgevoerd binnen overeengekomen onderhoudsvensters en tijdig aangekondigd, hierbij wordt ook gemeld waarop het onderhoud wordt uitgevoerd. Bij wijzigingen die leiden tot down-time van de applicatie wordt onderhoud altijd buiten kantooruren (na 18.00 uur) uitgevoerd en minimaal 5 werkdagen van tevoren aangekondigd. Bij spoedwijzigingen mag, in overleg met Opdrachtgever, hiervan worden afgeweken.	KO		

4. Governance en Samenwerking eisen

Governance en Samenwerking eisen				
Eis Governance en Samenwerking 4.1	Inschrijver werkt aantoonbaar samen met Aanbestedende Dienst en betrokken leveranciers door tijdige afstemming, informatievoorziening en deelname aan governance-overleggen.	KO		
Eis Governance en Samenwerking 4.2	Inschrijver neemt deel aan operationele, tactische en strategische overleggen conform overeengekomen governance afspraken.	KO		
Eis Governance en Samenwerking 4.3	Innovatie en continue verbetering maken onderdeel uit van de governance cyclus. Inschrijver en Aanbestedende Dienst evalueren periodiek technologische ontwikkelingen en optimalisaties.	KO		
Eis Governance en Samenwerking 4.4	Inschrijver stelt vaste contactpersonen beschikbaar voor operationeel, tactisch en strategisch niveau. En informeert aanbestedende dienst bij wijzigingen.	KO		
Eis Governance en Samenwerking 4.5	Inschrijver levert periodiek een roadmap voor lifecycle management en doorontwikkeling van de dienstverlening.	KO		
Eis Governance en Samenwerking 4.6	Inschrijver faciliteert kennisoverdracht en samenwerking tussen betrokken beheer- en ontwikkelteams.	KO		
Eis Governance en Samenwerking 4.7	Rollen, verantwoordelijkheden en afhankelijkheden worden vastgelegd in een gezamenlijk vastgesteld RACI-model tussen alle betrokken partijen	KO		
Eis Governance en Samenwerking 4.8	Inschrijver adviseert periodiek over relevante technologische ontwikkelingen en optimalisaties.	KO		
Eis Governance en Samenwerking 4.9	Inschrijver richt de dienstverlening zodanig in dat migratie naar een andere leverancier uitvoerbaar blijft. De dienstverlening ondersteunt: • open standaarden en indien relevant federatief datastelsel; • overdraagbaarheid; • exporteerbaarheid van data en configuraties; • actuele documentatie.	KO		
Eis Governance en Samenwerking 4.10	Inschrijver beschikt over een formeel escalatieproces voor operationele, tactische en strategische issues.	KO		

Eis Governance en Samenwerking 4.11	Governance afspraken over besluitvorming, wijzigingen en risicoacceptatie worden vastgelegd in het DAP en SLA. Jaarlijks worden het DAP en SLA geëvalueerd en indien nodig bijgesteld.	KO		
Eis Governance en Samenwerking 4.12	Dienstverlener biedt andere leveranciers van opdrachtgever toegang tot de omgevingen voor beheer en onderhoud. Hierbij gelden dezelfde afspraken als tussen dienstverlener en opdrachtgever onderling zijn afgesproken.			
Eis Governance en Samenwerking 4.13	Inschrijver is verplicht om binnen een multi-vendor omgeving te acteren.	KO		

5. Hosting- en Beheer eisen

Hosting- en Beheer eisen				
Eis Hosting en Beheer 5.1	De inschrijver levert een oplossing waarop de opdrachtgever haar applicaties (zie bijlages en Hoofdstuk 7. Applicaties) kan hosten en waarop ten minste de volgende componenten ondersteund en als geïntegreerde dienstverlening worden aangeboden: • Applicatieservers • RDS-servers • Webservers • Databaseclusters • Active Directory (AD)-servers • File (FS)-clusters • Mailrelays	KO		
Eis Hosting en Beheer 5.2	De aanbieder dient te waarborgen dat de oplossing voldoet aan de volgende beschikbaarheidseisen: Voor de productieomgeving geldt een beschikbaarheid van 99,0% gedurende het service window (maandag tot en met vrijdag van 08:00 tot 18:00 uur). Buiten dit service window (weekend en maandag tot en met vrijdag van 18:00 tot 08:00 uur) bedraagt de beschikbaarheid 97,5%. Voor de ontwikkel-, acceptatie- en testomgeving geldt een beschikbaarheid van 97,5% gedurende het service window (maandag tot en met vrijdag van 08:00 tot 18:00 uur). Buiten dit service window (weekend en maandag tot en met vrijdag van 18:00 tot 08:00 uur) wordt de beschikbaarheid geleverd op basis van <i>best effort</i>. De beschikbaarheid wordt gemeten en gerapporteerd als het deel van de tijd dat de hosting- en netwerk infrastructuur ten behoeve van de applicatie omgeving beschikbaar was t.o.v. de totale tijd in het service window 'Werkdagen'	KO		
Eis Hosting en Beheer 5.3	De aangeboden oplossing moet voldoende capaciteit en performance leveren om de op het platform gehoste applicaties en gegevensverwerkingen binnen de overeengekomen prestatieniveaus te kunnen uitvoeren. De inschrijver voorziet in actieve performance- en capaciteitsmonitoring en geeft opdrachtgever inzicht in het gebruik, de belasting, trends en eventuele capaciteitsknelpunten.	KO		

	Monitoring omvat minimaal compute, storage, netwerk, virtualisatie en kritieke infrastructuurdiensten.			
Eis Hosting en Beheer 5.4	Het platform ondersteunt Windows OS - en kan mogelijk Linux- ondersteunen	KO		
Eis Hosting en Beheer 5.5	De oplossing moet schaalbaar zijn door uitbreiding van CPU, geheugen, storage en netwerkcapaciteit De inschrijver geeft aan welke maximale capaciteit binnen de aangeboden oplossing beschikbaar is	KO		
Eis Hosting en Beheer 5.6	Inschrijver verzorgt het technisch beheer van de overeengekomen infrastructuur en platformdiensten inclusief (applicatie) monitoring en operationeel beheer.	KO		
Eis Hosting en Beheer 5.7	Inschrijver test periodiek fail-over- en back-upvoorzieningen en stelt resultaten beschikbaar aan opdrachtgever.	KO		
Eis Hosting en Beheer 5.8	Inschrijver richt geautomatiseerd logbeheer en logretentie in conform wet- en regelgeving en overeengekomen bewaartermijnen.	KO		
Eis Hosting en Beheer 5.9	Voor OTAP-omgevingen gelden passende logretentie- en opschoningsprocessen conform classificatie van gegevens.	KO		
Eis Hosting en Beheer 5.10	Inschrijver verleent medewerking aan performancetesten en ondersteunt opvolging van bevindingen binnen de eigen verantwoordelijkheid.	KO		
Eis Hosting en Beheer 5.11	De dienstverlening omvat bescherming tegen malware, virussen en schadelijke software. De software uit landen met een offensief cyberprogramma tegen Nederlandse belangen (zoals Rusland, China, Iran, Noord-Korea) is niet toegestaan	KO		
Eis Hosting en Beheer 5.12	Inschrijver levert en beheert alle benodigde licenties voor de overeengekomen dienstverlening.	KO		
Eis Hosting en Beheer 5.13	Inschrijver is verplicht ondersteuning aan te bieden voor veilige koppelingen met externe infrastructuur en dienstverlening van derden.	KO		
Eis Hosting en Beheer 5.14	De dienstverlening ondersteunt geografische redundantie tussen fysiek gescheiden datacenterlocaties.	KO		
Eis Hosting en Beheer 5.15	De dienstverlening omvat lifecycle-management van OS, database en middleware inclusief: • periodieke updates; • security patching; • gecontroleerde upgrades; • compatibiliteitsbeheer. Niet ondersteunde softwareversies mogen niet ongemerkt in productie blijven draaien. Changes worden uitgevoerd conform een formeel changeproces waarin opdrachtgever wordt geconsulteerd en geïnformeerd over de inhoud en impact van deze changes. De opdrachtgever ontvangt minimaal jaarlijks een overzicht in de lifecycle-status van de gebruikte technologie.	KO		
Eis Hosting en Beheer 5.16	Inschrijver monitort beschikbaarheid, capaciteit en technische gezondheid van de dienstverlening proactief.	KO		
Eis Hosting en Beheer 5.17	De dienstverlening ondersteunt aantoonbaar herstel van systemen, data en configuraties.	KO		
Eis Hosting en Beheer 5.18	De inschrijver zorgt voor een proces dat zorgdraagt voor kopieën van PRD op de OTA na een release volgens een afgesproken cadans (minimaal 2 keer per jaar). Opdrachtgever wordt op de hoogte gesteld van interne changes en de inhoud en impact van deze changes.	KO		

Eis Hosting en Beheer 5.19	Het platform moet schaalbare virtual machines (VM's) kunnen aanbieden met de volgende eisen: - Minimaal 2 vCPU en 4 GB RAM per VM voor de kleinste servers - Minimaal 12 vCPU en 256 GB RAM per VM moeten ondersteund worden om te voldoen aan de behoeften van de zwaarste workloads Daarnaast moet het platform flexibele schaalbaarheid bieden, zodat VM's binnen dit bereik (en eventueel daarbuiten) kunnen worden geconfigureerd op basis van de specifieke eisen van de applicaties.	KO		
Eis Hosting en Beheer 5.20	Inschrijver hanteert een gestructureerd lifecyclebeleid waarbij systemen en platformsoftware worden bijgehouden op versie n (meest actuele stabiele release) tot maximaal n-1 (de direct daaraan voorafgaande versie). Versies ouder dan n-1 zijn in productie niet toegestaan, tenzij Opdrachtgever hiervoor expliciet (schriftelijk) dispensatie verleent. Voor kritieke beveiligingsincidenten of kwetsbaarheden (geclassificeerd als <i>High/High</i> volgens de normen van het Nationaal Cyber Security Centrum (NCSC)) geldt dat de bijbehorende patch binnen 24 uur na beschikbaarstelling door de leverancier moet zijn geïnstalleerd en operationeel moet zijn. Bij kwetsbaarheden met een actieve exploit dient direct actie te worden ondernomen. Het definitieve patchbeleid wordt nader afgestemd met de opdrachtgever.	KO		

6. Architectuur eisen

Architectuur eisen				
Eis Architectuur 6.1	De oplossing ondersteunt monitoring, alerting en end-to-end ketenmonitoring, met bijbehorende tooling	KO		
Eis Architectuur 6.2	De Inschrijver draagt zorg voor een Low-level design (LLD) en High-level design (HLD) voor aanvang van de dienstverlening en onderhoud deze gedurende de gehele looptijd van de overeenkomst.	KO		
Eis Architectuur 6.3	De Architectuur ondersteunt scheiding tussen productie, test, acceptatie en ontwikkelomgevingen. (O)TAP-omgevingen zijn logisch en/of fysiek gescheiden ingericht.	KO		
Eis Architectuur 6.4	De inrichting van de OTAP-straat is zodanig dat deze, over omgevingen heen, gelijk is qua parameters. De inrichting van de AP-straat is zodanig dat het reproduceren van gemelde incidenten mogelijk is. De versie-en distributie inrichting is zodanig dat testresultaten reproduceerbare uitkomsten genereren in de TAP-straat.	KO		
Eis Architectuur 6.5	De architectuur ondersteunt netwerk-, tenant- en data-isolatie inclusief role-based toegangsbeheer.	KO		
Eis Architectuur 6.6	Inschrijver beschikt aantoonbaar over ervaring met: • virtualisatie; • bare-metal infrastructuur.	KO		
Eis Architectuur 6.7	De oplossing ondersteunt voor CI/CD processen om de implementaties, updates en beheer van de oplossingen te automatiseren. De leverancier dient aan te tonen dat: Het platform compatibel is met versiebeheersystemen en (declaratief) configuratiebeheer. Wijzigingen aan	KO		

	infrastructuur en applicaties automatisch kunnen worden gesynchroniseerd met de werkelijke omgeving. Alle deployments auditbaar en herhaalbaar zijn, met ondersteuning voor rollbacks en compliance-rapportage			
Eis Architectuur 6.8	Inschrijver past moderne beheerprincipes toe gericht op automatisering, betrouwbaarheid en schaalbaarheid, zowel op -als afschalen. Kosten en resourceverbruik zijn inzichtelijk en herleidbaar.	KO		
Eis Architectuur 6.9	De oplossing ondersteunt hybride infrastructuurmodellen en integratie met verschillende hostingomgevingen.	KO		
Eis Architectuur 6.10	De architectuur ondersteunt redundantie over meerdere fysiek gescheiden datacenterlocaties.	KO		
Eis Architectuur 6.11	Architectuur ondersteunt schaalbare opslag en compute-capaciteit	KO		
Eis Architectuur 6.12	Inschrijver neemt deel aan periodieke architectuur overleggen en ondersteunt doorontwikkeling binnen overeengekomen scope.	KO		
Eis Architectuur 6.13	De architectuur ondersteunt netwerksegmentatie en veilige scheiding tussen intern en extern verkeer conform gangbare architectuurprincipes.	KO		
Eis Architectuur 6.14	De oplossing ondersteunt veilige en flexibel configureerbare koppelingen met externe systemen.	KO		
Eis Architectuur 6.15	Inschrijver heeft bij de oplossing een voorkeur voor open standaarden en breed ondersteunde open-source componenten.	KO		
Eis architectuur 6.16	De inrichting van de oplossing is een geïntegreerde totaaloplossing waarbij alle modules gebruik maken van dezelfde gegevens volgens het principe 'eenmalige registratie/meervoudig gebruik'.	KO		
Eis architectuur 6.17	De oplossing is schaalbaar en ondersteunt groei (en afschaling) in aantal administraties, gebruikers en transacties (CPU, geheugen, storage e.d.)	KO		
Eis architectuur 6.18	De opdrachtnemer documenteert en de ondersteunde architectuur en softwareversies en koppelt hier periodiek (en na changes) op terug aan opdrachtgever.	KO		
Eis architectuur 6.19	Het platform biedt ondersteuning voor meerdere authenticatiemethoden: • Entra ID (/WAAD) voor applicaties die dit ondersteunen • Lokale active directories (AD) voor applicaties die niet federatief kunnen koppelen en afhankelijk zijn van lokale accounts Gebruikers die zowel Synergy als Globe+ gebruiken, moeten met hetzelfde account kunnen inloggen in beide systemen. In de toekomst zal dit mogelijk wijzigen waarop deze afspraak aangepast zal worden.	KO		
Eis architectuur 6.20	Verantwoordelijkheid voor het up-to-date houden van de rechten in de AD ligt bij de Opdrachtgever. Opdrachtnemer werkt mee aan het 3-maandelijks controleren van uitgegeven autorisaties.	KO		

7. Applicaties eisen

Applicaties eisen				
Eis Applicaties 7.1	Inschrijver werkt gedurende de uitvoering van de Overeenkomst samen met huidige leveranciers van Aanbestedende Dienst voor zover dit noodzakelijk is voor een goede uitvoering van de dienstverlening.	KO		
Eis Applicaties 7.2	Het platform moet onderstaande applicaties kunnen hosten en kunnen voldoen aan de aanbevolen systeemeisen	KO		

	passend bij het aantal (gelijktijdige) gebruikers, databaseomvang en belasting voor: • Exact Globe+ • Exact Synergy (inclusief add-on Cifas en Edd-on bouwstenen) • BPA Platform • TimeXtender • Qlik Sense • Qlik NPrinting			
Eis Applicaties 7.3	De applicaties binnen de oplossing werken naar tevredenheid van gebruikers. Het op- en afschalen van resources is hiervoor mogelijk. De Inschrijver dient aan te tonen hoe de aangeboden infrastructuur en configuratie bijdragen aan het behalen van de performance-eisen zoals deze gelden. Hiertoe wordt voorafgaand aan implementatie een meetmethodiek vastgesteld, inclusief tooling, meetmomenten en acceptatiecriteria.	KO		
Eis Applicaties 7.4	Compliance & audits: • Verwerkersovereenkomst; • Jaarlijkse ISAE3402 type II rapportage van de leverancier.	KO		
Eis Applicaties 7.5	De aangeboden oplossing dient tooling te bieden voor centrale en geïntegreerde monitoring, logging en visualisatie (dashboards) van platform- en applicatiegegevens die op verzoek ook inzichtelijk zijn voor opdrachtgever.	KO		
Eis Applicaties 7.6	De aangeboden oplossing dient ondersteuning te bieden voor: • het geautomatiseerd en reproduceerbaar uitrollen van applicaties en bijbehorende configuraties; • het kunnen definiëren en beheren van uitbreidingen op de standaard platformfunctionaliteit; • het betrouwbaar uitvoeren en beheren van zowel stateless als stateful applicatie-componenten, inclusief opslag-intensieve processen.	KO		
Eis Applicaties 7.7	De aangeboden oplossing dient ondersteuning te bieden voor gestandaardiseerde mechanismen routing van verkeer, zodanig dat bestaande configuraties zonder ingrijpende aanpassingen kunnen worden voortgezet.	KO		
Eis Applicaties 7.8	De aangeboden oplossing dient te voorzien in logging die centraal ontsloten, doorzoekbaar en beschikbaar is voor de opdrachtgever en applicatiebeheerpartij van, zodat beheer, troubleshooting en analyse zonder belemmeringen kunnen plaatsvinden. Voor het applicatiebeheer wordt verwacht dat er één hoofdaanspreekpunt is, kennis dient bij meerdere personen belegd te zijn zodat er altijd achtervang is ingeregeld.	KO		
Eis Applicaties 7.9	Bewaartermijnen voor logging worden vastgesteld op basis van een risicoafweging volgens de BIO en het noodzakelijkheidbeginsel uit de AVG. Afhankelijk van het doel (bijv. detectie, forensisch onderzoek, audit) kunnen verschillende bewaartermijnen gelden.	KO		
Eis Applicaties 7.10	De aangeboden oplossing dient geschikt te zijn voor het beheren van meerdere omgevingen, waarbij: • Role-based access control omgeving kan worden ingericht; • Centrale governance over meerdere omgevingen mogelijk is.	KO		
Eis Applicaties 7.11	De inschrijver dient in staat te zijn om een client-server applicatie te hosten op het platform. Inclusief de installatie, configuratie, onderhoud en beveiliging daarvan.	KO		
Eis Applicaties 7.12	Het platform biedt de mogelijkheid om de servercomponent te installeren op een dedicated of shared VM of fysieke server met ondersteuning voor Microsoft Windows Server en Microsoft SQL Server 2022 of hoger.	KO		

	Opdrachtnemer moet garanties bieden voor de ondersteuning van toekomstige versies van deze software, zodra de applicaties deze vereisen.			
Eis Applicaties 7.13	De inschrijver dient in staat te zijn om de client applicatie beschikbaar te stellen op de werkplekvoorziening van de eindgebruiker d.m.v. beveiligde remote toegang	KO		
Eis Applicaties 7.14	De remote toegang oplossing moet schaalbaar zijn naar minimaal 100 gelijktijdige Exact Globe-gebruikers, waarbij uitbreiding met aanvullende servers mogelijk moet zijn.	KO		
Eis Applicaties 7.15	Toegang tot de remote toegang -omgeving mag niet rechtstreeks via het publieke internet beschikbaar worden gesteld en moet plaatsvinden via een beveiligde toegangsdienst De remote toegang dient waar mogelijk gekoppeld te worden aan de SSO-Rijk en DWR 2.0. Waar dit niet mogelijk is wordt gebruik gemaakt van een stepping stone met 2FA.	KO		
Eis applicaties 7.16	De (remote toegang) servers zijn voorzien van de Office-onderdelen die vanuit de applicaties nodig zijn. Versie: 64 bit installatie van Office 2024 met Word en Excel (en het openen van .msg bestanden).	KO		
Eis Applicaties 7.17	De omgeving moet voldoende capaciteit en schaalbaarheid bieden om het maximale aantal gelijktijdige Exact Synergy gebruikers per webserver (gemeten per 5-minuteninterval) te ondersteunen. De capaciteit moet worden gegarandeerd voor piekmomenten en rekening houden met een buffer van minimaal 20% boven op de opgegeven aantallen om onvoorziene pieken op te vangen. Het gemiddeld aantal gelijktijdige gebruikers per 5 minuten varieert binnen een bandbreedte van 20 tot 100 gelijktijdige gebruikers per 5 minuten per webserver	KO		
Eis Applicaties 7.18	De omgeving moet voldoende capaciteit bieden om 50 gelijktijdige Qlik Sense gebruikers te ondersteunen met de mogelijkheid dit uit te breiden	KO		
Eis Applicaties 7.19	De webapplicaties zijn benaderbaar via de meest gangbare webbrowsers (minimaal (Edge) Chromium en Firefox browsers)	KO		

8. Integraties eisen

Integratie eisen				
Eis Integraties 8.1	Het platform moet netwerkconnectiviteit met externe systemen ondersteunen	KO		
Eis Integraties 8.2	Integraties moeten via beveiligde verbindingen verlopen volgens de relevante open standaarden van Forum Standaardisatie	KO		
Eis Integraties 8.3	Het platform biedt de mogelijkheid om veilig gegevens uit te wisselen met externe systemen en partijen via API's of webhooks. Er wordt de mogelijkheid geboden om API-uitwisseling te loggen en te authentifieren via een token.	KO		
Eis Integraties 8.4	De oplossing ondersteunt bij het beschikbaarstellen (importen en exporteren) van bestanden via veilige netwerkshares (bijv. SFTP)	KO		
Eis Integraties 8.5	Het platform ondersteunt bij batchverwerkingen buiten service windows (o.a. voor overzetten dataloads van Exact databases naar DWH)	KO		

Eis Integraties 8.6	Het platform ondersteunt geautomatiseerde bestandsuitwisseling via scheduled tasks (bijv. windows import taken) voor periodieke import/export.	KO		
Eis Integraties 8.7	De oplossing ondersteunt een VPN-aansluiting op een Equinix datacenter	KO		
Eis Integraties 8.8	De oplossing ondersteunt aansluiting op de Haagse Ring VPN van SSC-ICT	KO		
Eis Integraties 8.9	De oplossing ondersteunt op termijn bij aansluiting op de Haagse Ring VPN van DICTU	KO		
Eis Integraties 8.10	De oplossing moet integratie met de bestaande identity en serviceprovider van de opdrachtgever ondersteunen	KO		
Eis Integraties 8.11	De oplossing biedt de mogelijkheid om uitgaande e-mail te routeren via een geconfigureerd extern mailrelay (SMTP-relay) van de opdrachtgever.	KO		

9. Archivering eisen

Archivering Eisen				
Eis archivering 9.1	Opdrachtnemer kan een centrale archiveringsfunctionaliteit bieden die het mogelijk maakt om archiefwaardige gegevens uit de productiedatabases op een veilige, gestructureerde en toegankelijke wijze te verplaatsen naar een gescheiden archiefomgeving.	KO		
Eis archivering 9.2	Gearchiveerde gegevens en documenten moeten door geautoriseerde gebruikers kunnen worden geraadpleegd zonder dat deze gegevens opnieuw in de productieomgeving hoeven worden opgenomen.	KO		
Eis archivering 9.3	De archiefoplossing moet gebruikers in staat stellen gearchiveerde gegevens en documenten te zoeken en te filteren op administratie	KO		

10.Back-up en herstel eisen

Back-up en herstel eisen				
Eis back-up 10.1	Het platform moet automatische back-ups ondersteunen, met configuratieopties voor frequentie, retentie en segmentatie	KO		
Eis back-up 10.2	De inschrijver dient voor productiedata een RPO van maximaal 8 aaneengesloten uren te realiseren. De back-up strategie dient zo ingericht te zijn dat altijd een herstelpunt beschikbaar is dat maximaal 8 uur oud is.	KO		
Eis back-up 10.3	De opdrachtnemer dient de productieomgeving na een calamiteit binnen maximaal twee werkdagen (RTO) te herstellen	KO		
Eis back-up 10.4	De inschrijver dient de acceptatieomgeving na een calamiteit binnen maximaal vier werkdagen (RTO) te herstellen.	KO		
Eis back-up 10.5	Alle voor herstel noodzakelijke configuraties, scripts, instellingen, infrastructuurdefinities, koppelingen en documentatie dienen geback-up't en/of reproduceerbaar opgeslagen te worden	KO		
Eis back-up 10.6	De leverancier dient een retentiebeleid te bieden waarmee herstel mogelijk is naar zowel recente herstelpunten als historische herstelpunten. De inschrijver dient de voorgestelde retentie expliciet te beschrijven en af te stemmen met de opdrachtgever	KO		

Eis back-up 10.7	Opdrachtnemer heeft een duidelijk herstelplan voor serverherstel en communiceert deze met de opdrachtgever. Opdrachtnemer gaat pas na expliciet akkoord van de opdrachtgever over tot het terugplaatsen van een back-up.	KO		
Eis back-up 10.8	Opdrachtnemer voert minstens een keer per jaar een integrale recovery/restore test uit waarbij wordt getest of het lukt om de RPO en RTO te halen. Opdrachtnemer rapporteert hierover naar de opdrachtgever	KO		
Eis back-up 10.9	Alleen geautoriseerd personeel heeft toegang tot de back-up data.	KO		
Eis back-up 10.10	Inschrijver bewaakt en controleert de werking van back-upvoorzieningen en rapporteert hierover periodiek naar opdrachtgever.	KO		
Eis back-up 10.11	Het back-upnetwerk wordt fysiek gescheiden van het productienetwerk	KO		
Eis back-up 10.12	De back-up wordt opgeslagen op een fysiek gescheiden geografische locatie	KO		

11.Migratie eisen

Migratie eisen				
Eis Migratie 11.1	Inschrijver hanteert een aantoonbare migratieaanpak gericht op: • continuïteit van dienstverlening; • beperking van verstoringen; • minimale noodzakelijke aanpassingen aan applicaties en configuraties.	KO		
Eis Migratie 11.2	Migraties worden uitgevoerd met minimale impact op beschikbaarheid van dienstverlening.	KO		
Eis Migratie 11.3	OTAP-omgevingen worden gecontroleerd en gefaseerd gemigreerd conform overeengekomen migratieplanning.	KO		
Eis Migratie 11.4	De migratieaanpak omvat: • kennisoverdracht; • gecontroleerde overgangsfasen; • overdracht van beheer- en architectuur documentatie.	KO		
Eis Migratie 11.5	Voorafgaand aan migratie wordt een risicoanalyse uitgevoerd inclusief beheersmaatregelen en fallbackscenario's.	KO		
Eis Migratie 11.6	End-of-life componenten worden voorafgaand aan of tijdens migratie geïnventariseerd en voorzien van passende mitigerende maatregelen of vervanging.	KO		
Eis Migratie 11.7	Inschrijver stelt voorafgaand aan migratie een migratieplan op inclusief: • fasering; • risicoanalyse; • fallbackscenario's; • testaanpak; • communicatiestructuur.	KO		
Eis Migratie 11.8	De migratieaanpak ondersteunt gecontroleerde terugvalscenario's bij verstoringen of mislukte migratiestappen.	KO		
Eis Migratie 11.9	Productie-ingebruikname vindt plaats na gezamenlijke acceptatie van overeengekomen test- en migratieresultaten.	KO		
Eis Migratie 11.10	Inschrijver borgt overdracht van kennis, configuraties en documentatie gedurende de migratieperiode.	KO		

12.Innovatie eisen

Innovatie eisen

Eis Innovatie eisen 12.1	Inschrijver levert periodiek voorstellen voor optimalisatie van dienstverlening, beheer, beveiliging of kostenbeheersing	KO		
Eis Innovatie eisen 12.2	Inschrijver en Aanbestedende Dienst evalueren periodiek technologische ontwikkelingen en mogelijke verbeteringen van de dienstverlening	KO		
Eis Innovatie eisen 12.3	Voorstellen voor doorontwikkeling sluiten aan op: • beleidsdoelstellingen; • beveiligings- en compliance-eisen; • architectuur- en soevereiniteitskaders.	KO		
Eis Innovatie eisen 12.4	Inschrijver ondersteunt samenwerking gericht op continue optimalisatie van dienstverlening.	KO		
Eis Innovatie eisen 12.5	Inschrijver adviseert periodiek over technologische vernieuwing en lifecycle management van infrastructuur en hostingdiensten.	KO		
Eis Innovatie eisen 12.6	Inschrijver adviseert periodiek, elk kwartaal, over optimalisatie van: • prestaties; • schaalbaarheid; • beschikbaarheid; • kosten van de dienstverlening.	KO		
Eis Innovatie eisen 12.7	Inschrijver informeert opdrachtgever periodiek over relevante technologische ontwikkelingen die impact kunnen hebben op de dienstverlening.	KO		
Eis Innovatie eisen 12.8	Inschrijver levert periodiek een roadmap voor technologische doorontwikkeling van de dienstverlening.	KO		
Eis Innovatie eisen 12.9	Inschrijver adviseert proactief over lifecycle-risico's en noodzakelijke modernisering.	KO		
Eis Innovatie eisen 12.10	Inschrijver ondersteunt verdere automatisering van beheer, waaronder onder andere geautomatiseerd testen, RPA, AI - en deployment processen	KO		
Eis Innovatie eisen 12.11	Inschrijver en Aanbestedende Dienst evalueren periodiek mogelijke verbeteringen op gebied van: • beschikbaarheid; • beveiliging; • beheerbaarheid; • monitoring; • kosten; • schaalbaarheid.	KO		
Eis Innovatie eisen 12.12	Inschrijver kan Aanbestedende Dienst ondersteunen bij het eventueel overstappen van client applicaties naar webapplicaties of opensource software.	KO		

13.SIEM/SOC (Optioneel)

SIEM/SOC eisen

Eis SIEM/SOM 13.1	Aanbod voor de afname van een SOC-voorziening wordt opgeleverd door Opdrachtnemer. Dienst wordt meegenomen in de offerteaanvraag, maar afname is optioneel.	KO		
Eis SIEM/SOM 13.2	SOC voorziening voldoet aan: • 24/7 eyes on screen • Heldere definitie van aan te sluiten logbronnen • Triage aan de voorkant door opdrachtnemer • Heldere afspraken over detectie- en responsetijden • Heldere afspraken over samenwerking, rules of engagement en escalatie • Opslag logbronnen conform AVG, mogelijkheid tot forensisch onderzoek en maximaal 1 jaar • SOC is schaalbaar met de omgeving • Maandelijkse rapportage en doorspreken van incidenten met een SOC-analist	KO		

Eis SIEM/SOM 13.3	Indien Opdrachtgever besluit de SIEM/SOC-dienstverlening niet af te nemen bij Opdrachtnemer (bijvoorbeeld vanwege de inzet van een eigen voorziening of een Rijksbrede SOC-voorziening), is Opdrachtnemer verplicht om zonder meerkosten de benodigde interfaces, logging-stromen en API-koppelingen beschikbaar te stellen ten behoeve van aansluiting op de door Opdrachtgever aangewezen externe voorziening.	KO		
-------------------	--	----	--	--

14. Maatschappelijk Verantwoord Opdrachtgeven en Inkopen (MVOI)

Migratie eisen				
Eis MVOI 14.1	Klimaat De datacentra die worden aangewend voor de uitvoering van de Opdracht hebben een Power Usage Effectiveness (PUE) van maximaal 1,3. De PUE wordt berekend conform erkende methodes zoals beschreven in ISO IEC 30134-2. De ook wel gehanteerde Datacenter infrastructure Efficiency (DCiE) komt overeen met 1/PUE. Een DCiE van 1,3 staat dus gelijk aan een PUE van 76,9%.	KO		
Eis MVOI 14.2	Opdrachtnemer spant zich actief in op het gebied van het continue ontwikkelen en uitdragen van aantoonbare relevante competenties en ervaring in het optimaliseren van software met het doel om energieverbruik te minimaliseren.	KO		
Eis MVOI 14.3	Circulair Bij de uitvoering van de opdracht wordt afgedankte hardware (uit de datacentra) hoogwaardig hergebruikt of als dat niet mogelijk is, wordt deze gerecycled. Dit in het kader van circulariteit.	KO		
Eis MVOI 14.4	Social return 2.0 Het is de taak van de overheid om mensen met een afstand tot de arbeidsmarkt te ondersteunen. Zodat iedereen zoveel mogelijk meedoet in de samenleving en uitzicht houdt op werk en inkomen, zie de website voor meer achtergrondinformatie. Wij vinden social return belangrijk en willen graag impact creëren en tegelijkertijd dat het proportioneel blijft. Daarom geven wij Opdrachtnemer de mogelijkheid een vrije invulling aan social return te geven. Dit mag zowel direct als indirect verband houden met de opdracht. Opdrachtnemer spant zich in om tenminste 1% van de gerealiseerde opdrachtwaarde gedurende de looptijd van de Overeenkomst te besteden aan een nieuw social return initiatief of een uitbreiding van een bestaand initiatief. Onder mensen met een afstand tot de arbeidsmarkt wordt verstaan: 1. Langdurig werkzoekenden (langer dan 12 maanden); 2. Mensen die langer dan 12 maanden niet aan het werk zijn en aanspraak maken op een uitkering vanuit de overheid; 3. Mensen die anderszins zonder (re-integratie) ondersteuning of begeleiding niet of lastig zelfstandig aan werk kunnen komen (denk daarbij bijvoorbeeld aan jongeren met onvoldoende kwalificaties, ouderen 50+ met onvoldoende kwalificaties, statushouders, ex-gedetineerden).	KO		

	Let op! Mensen die nu reeds betaald werk verrichten, waaronder huidige werknemers van Opdrachtnemer behoren uitdrukkelijk niet tot de doelstelling/doelgroep van deze Aanbesteding. <u>Plan van aanpak social return</u> Opdrachtnemer maakt na (voorlopige) gunning een Plan van aanpak social return en dient dit binnen één maand na ingangsdatum van de Overeenkomst in. In dit plan van aanpak beschrijft Opdrachtnemer hoe hij social return gaat toepassen bij de uitvoering van de Overeenkomst. Het plan van aanpak bevat in ieder geval: • De wijze waarop u impact creëert; • De manier waarop u het afgesproken percentage realiseert; • De wijze waarop u de begeleiding vormgeeft, indien van toepassing op uw initiatief; • De randvoorwaarden; • De planning. De Opdrachtgever keurt het Plan van aanpak social return goed of vraagt om een verbetering. Na akkoord op uw Plan van aanpak social return is Opdrachtnemer verplicht om binnen twee (2) maanden te starten met de uitvoering ervan. Dit goedgekeurde Plan van aanpak social return wordt een onderdeel van de Overeenkomst. De invulling moet controleerbaar zijn en wordt minimaal jaarlijks besproken met de Opdrachtgever. Voor de verantwoording maakt Opdrachtnemer gebruik van het online systeem Wizzr, waartoe Opdrachtnemer van Opdrachtgever toegang krijgt.			
Eis MVOI 14.5	Digitale toegankelijkheid Opdrachtnemer zal de Digitale toegankelijkheid stimuleren, op grond van de Europese richtlijn voor toegankelijkheid van overheidswebsites en -apps, die is omgezet in Nederlandse wetgeving: 'toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties'.	KO		
Eis MVOI 14.6	Diversiteit & Inclusie Opdrachtnemer neemt kennis van het 'Charter Diversiteit' van Diversiteit in Bedrijf en spant zich in om diversiteit en inclusie op de werkvloer te bevorderen.	KO		
Eis MVOI 14.7	Impact realiseren met Open Source Software (OSS) Opdrachtnemer stimuleert de inzet van open source software die maatschappelijke meerwaarde oplevert. Dit kan bijvoorbeeld door zelf activiteiten uit te voeren, zoals het ontwikkelen of verbeteren van open source software, of door het uitbesteden van maatschappelijke bijdragen, zoals via een donatie aan een erkend open source initiatief. Hieronder volgt een aantal voorbeelden: <u>Bijdragen aan bestaande open source projecten</u> Dit omvat het oplossen van bugs, ontwikkelen van nieuwe functionaliteiten, verbeteren van documentatie of het leveren van support aan open source projecten met maatschappelijke relevantie. <u>Vrijgeven van nieuwe open source software</u> Indien Opdrachtnemer in het kader van deze opdracht (maatwerk) software of modules ontwikkelt die herbruikbaar	KO		

	zijn, dan kunnen deze componenten als open source software te worden vrijgegeven onder een OSI-gecertificeerde licentie (na voorafgaande schriftelijke toestemming van de opdrachtgever). <u>Donaties aan bestaande open source initiatieven</u> Donaties aan één of meerdere (internationaal) erkende op open source gerichte non-profit stichtingen of verenigingen, zoals NLnet en de Sovereign Tech Agency.			
--	--	--	--	--

15. Gevolgen van niet naleving

De eisen uit het Programma van Eisen maken onderdeel uit van de Overeenkomst en dienen gedurende de looptijd van de Overeenkomst te worden nageleefd.

Indien tijdens de uitvoering van de Overeenkomst blijkt dat niet wordt voldaan aan één of meerdere eisen uit het Programma van Eisen, geldt dit als een tekortkoming in de nakoming van de Overeenkomst.

De Aanbestedende Dienst is in dat geval gerechtigd de Opdrachtnemer in de gelegenheid te stellen het gebrek binnen een redelijke termijn te herstellen.

Indien herstel uitblijft, of indien sprake is van een ernstige tekortkoming, is de Aanbestedende Dienst gerechtigd de Overeenkomst geheel of gedeeltelijk te ontbinden, onverminderd overige rechten van de Aanbestedende Dienst.