



VOORUITKIJKEN

EXTRA ONDERZOEK NAAR DOCUMENT MANAGEMENT,
RECORDS MANAGEMENT EN PROCESONDERSTEUNING
OPLOSSINGEN VOOR HET MINISTERIE VAN
INFRASTRUCTUUR EN WATERSTAAT





Utrecht, 18 december 2023
Versie 1.0

QA Consulting:
– André Nadorp

INHOUDSOPGAVE

1

Inleiding

2

Achtergrond

Een toelichting op de uitdagingen, de door lenW/ geschetste oplossingsruimte en de onderzoeksaanpak.

3

Leveranciers perspectief

Hoe kijkt de markt naar de beveligingsuitdaging van lenW/ binnen de gestelde oplossingsruimte.

4

Conclusies, aanbevelingen

Wat zijn op basis van de onderzoeksvragen en -resultaten de belangrijkste conclusies en aanbevelingen?

5

Wenkend perspectief

Op basis van het onderzoek, en onze algemene ervaring en kennis, wordt een wenkend perspectief geschetst.

6

Bijlagen

Een overzicht van de gebruikte afkortingen, een nadere toelichting op de oplossingsruimte en gebruikte documentatie.

1

Inleiding

Inleiding

1

Achter-
grond

2

Leveranciers-
perspectief

3

Conclusies &
Aanbevelingen

4

Wenkend
perspectief

5

Bijlagen

6

UITDAGINGEN N.A.V. EXTRA OPGESTELDE BEVEILIGINGSEISEN

1. Management-samenvatting

Achtergrond

Leveranciers perspectief

Conclusies

Aanbevelingen

Het ministerie van Infrastructuur en Waterstaat (IenW) maakt gebruik van verschillende Document Management Systemen (DMS). Deze DMS en Records Management Applicaties (RMA) zijn op aspecten verschillend, maar kennen vergelijkbare uitdagingen:

1. Verbeteren van de informatiehuishouding (IHH);
2. Invoering van nieuwe wet- en regelgeving;
3. Verbeteren van gebruiksvriendelijkheid;
4. Technologische verbeteringen.

Gegeven deze uitdagingen is er een oplossingsruimte gedefinieerd, die aangeeft wat de gewenste functionaliteit is. In beginsel gaat het dan om een DMS-RMA, waarbij documenten worden gecreëerd, opgeslagen, beheerd en geraadpleegd op basis van geautoriseerde toegang. Aanvullend is een aantal bouwblokken gevraagd, inclusief procesondersteuning bij het tot stand komen van de documenten.

Om inzicht te krijgen in wat de markt de departementen op deze punten te bieden heeft en of er een realistisch implementatiepad voor is, is in 2022 onderzocht waar men rekening mee dient te houden.

Op basis van recente ontwikkelingen zijn er extra vragen gedefinieerd door IenW met als centrale vragen:

- Welke Service- en implementatiemodellen zijn er mogelijk binnen de gestelde kaders? Is samenwerking met ODC Noord en implementatie op de Rijkscloud mogelijk en hoe werkt dit?
- Hoe kijkt de markt naar de uitdaging van IenW met betrekking tot beveiligingseisen?
- Welke samenwerking is mogelijk binnen verschillende service- en implementatiemodellen waarbij IenW optimaal ontzorgd wordt?

Dit rapport wordt hiermee een bijlage van de eerste marktverkenning.

2 Achtergrond

Wat is de aanleiding voor dit extra (verkorte) onderzoek, wat is de context en wat is de door de departementen gedefinieerde oplossingsruimte?

Inleiding

1

Achter-
grond

2

Leveranciers-
perspectief

3

Conclusies &
Aanbevelingen

4

Wenkend
perspectief

5

Bijlagen

6

EXTRA EISEN, ZELFDE DOELSTELLING

2. Achtergrond

Aanleiding

Het ministerie van Infrastructuur en Waterstaat (IenW) heeft na intern onderzoek de beveiligingseisen voor de te verwerven omgeving aangescherpt en op basis hiervan zijn er verdiepvragen opgesteld. Deze vragen gaan over:

1. Service en implementatiemodel
2. Informatiebeveiliging
3. Additionele dienstverlening

Gezien de additionele beveiligingseisen heeft IenW extra vragen gedefinieerd en aan de markt verzonden.

Om inzicht te krijgen in wat de markt de departementen op deze punten te bieden heeft en of er een realistische oplossing is, is onderzocht waar men rekening mee dient te houden. Met als centrale vragen:

- Welke Service- en implementatiemodellen zijn er mogelijk binnen de gestelde kaders? Is samenwerking met ODC Noord en implementatie op de Rijkscloud mogelijk en hoe werkt dit?
- Hoe kijkt de markt naar de uitdaging van IenW met betrekking tot beveiligingseisen?
- Welke samenwerking is mogelijk binnen verschillende service- en implementatiemodellen waarbij IenW optimaal ontzorgd wordt?

3 Leveranciers perspectief

Hoe kijkt de leveranciers naar de beveiligingsuitdagingen van IenW.

Inleiding

1

Achter-
grond

2

Leveranciers-
perspectief

3

Conclusies &
Aanbevelingen

4

Wenkend
perspectief

5

Bijlagen

6

Bijlagen



VERDIEPINGSVRAGEN OP DE BEVEILIGINGSUITDAGING VAN IENW

4. Leveranciersperspectief

Inleiding

Service- en
implementatiemodel

Informatiebeveiliging

Implementatie

Additionele dienstverlening

Dit hoofdstuk geeft een uiteenzetting van de antwoorden van de leveranciers op de vragen van IenW.

De verdiepingsvragen hebben als doel IenW meer inzicht te geven in welke mate de markt kan voldoen aan de aangescherpte eisen m.b.t. het beveiligingsniveau. De oplossingsruimte gaat in op de volgende elementen:

1. Service- en implementatiemodel: Een servicemodel geeft aan waar het beheer belegd is. Antwoorden op de vragen dienen inzicht te geven in de mogelijkheden van service- en implementatiemodellen waarbij Rijkscoud het uitgangspunten is .
2. Informatiebeveiliging: Met de vragen wil IenW meer inzicht krijgen in mogelijke ondersteuning bij het beveiligingsniveau BBN3 en de eventuele afhankelijkheden met de door leveranciers ondersteunde service- en implementatiemodellen.
3. Additionele dienstverlening: Met de antwoorden op de vragen wil IenW inzicht krijgen in welke meerwaarde uit aanvullende dienstverlening is te halen.

RIJKSCLOUD GEEN BEPERKING VOOR OPLOSSING

4. Leveranciersperspectief

Inleiding

Service- en
implementatiemodel

Informatiebeveiliging

Implementatie

Additionele dienstverlening

1. Is uw oplossing in te richten op het implementatiemodel RijkscLOUD en wordt hiermee de garantie gegeven dat de oplossing nu en in de toekomst door leverancier actueel gehouden wordt?

De meeste leveranciers geven aan dat ze de geboden oplossing kunnen inrichten op de RijkscLOUD en garanderen dat deze toekomstvast is. Bij een van de partijen wordt aangegeven dat het leveringsmodel intern nog uitgewerkt moet worden.

Leveranciers geven in de beantwoording niet aan wie de integratie verantwoordelijkheid heeft tussen de RijkscLOUD en hun oplossing.

2. Kan de oplossing in samenwerking met RijkscLOUD in een, voor het ministerie complementaire dienstverlening, als ware het een voor lenW SaaS dienstverlening aangeboden worden?

Leveranciers geven aan dat dit mogelijk is. Wel wordt er op gewezen dat hiervoor leveringsvoorwaarden tussen partijen afgesproken moeten worden.

3. Bent u bereid, gegeven de leveringsvoorwaarden van ODC Noord, om een continue dienstverlening te garanderen voor de gevraagde oplossing conform vraag 2?

Leveranciers zijn bereid om een continue dienstverlening te garanderen. Hierbij wordt er gewezen op het opstellen van nadere afspraken met ODC-Noord.

4. Welke servicemodellen zijn er mogelijk op het implementatiemodel RijkscLOUD als standaard dienstverlening?

Door leveranciers worden verschillende modellen aangeboden. Dit gaat van IaaS, waarbij het beheer van de oplossing geheel bij lenW komt te liggen, tot FaaS, waarbij het afrekenmodel op basis van gebruik gaat en lenW volledig ontzorgd wordt.

Op hoofdlijnen lopen de servicemodellen van Eigen beheer tot Managed services. Alle leveranciers kunnen de omgeving, onder voorwaarden, voor lenW beheren.

5. Welke dienstverlening is er mogelijk op het implementatiemodel RijkscLOUD?

Leverancier geven aan verschillende diensten te kunnen leveren op het implementatiemodel RijkscLOUD. Dit loopt van Technisch beheer tot en met het leer- en verandermanagement. Een leverancier geeft aan hier nog intern onderzoek naar te doen.



BBN3 REFERENTIES ZIJN ER, SLECHTS OP HOOFDLIJNEN BESCHREVEN

4. Leveranciersperspectief

Inleiding

Service- en
implementatiemodel

Informatiebeveiliging

Implementatie

Additionele dienstverlening

7. Kunt u referenties aandragen waarbij u te maken heeft met BBN3 (of vergelijkbaar) in de Europese publieke sector en kunt u daarbij aangeven welke service- implementatiemodellen daarop van toepassing zijn?

Leveranciers zijn terughoudend in het aandragen van referenties gezien het feit dat het hier gaat over BBN3 gerelateerde systemen. Een leverancier geeft geen antwoord op deze vraag.

Namen die gegeven worden (zonder inhoud van dienstverlening):

- Autoriteit persoonsgegevens
- ECB
- NATO
- Europese commissie
- Defensie1

8. Wat is uw visie en aanpak m.b.t. BBN3 (of vergelijkbaar) in relatie met de geboden oplossing en gewenste dienstverlening?

Deze vraag lijkt voor een aantal leveranciers moeilijk om te beantwoorden.

De twee die hier op ingaan geven de volgende feedback.

Leveranciers geven aan in gesprek te willen met lenW om de specifieke onderdelen van BBN3 af te stemmen en, indien mogelijk, te implementeren. Tevens worden verschillende

beveiligingsmaatregelen voorgesteld waarbij ook de gebruiker aan de hand wordt genomen. Hierbij is kennis en eigenaarschap bij lenW van belang. Het inrichten van processen om hier aan te blijven werken wordt door leveranciers als belangrijk ervaren.

In de aanpak wordt door deze beide leveranciers een gestructureerde fasering voorgesteld waarbij inzicht en inrichting nauw samengaan en continu gemonitord worden. Uit de beantwoording wordt niet duidelijk hoe de beveiliging van koppelingen naar generieke componenten (bv. Word) is ingericht.

9. Indien uw oplossing de mogelijkheid tot samenwerking tussen departementen in combinatie met het beveiligingsniveau BBN3 biedt, kunt u aangeven aan welke voorwaarden voldaan moet worden?

De oplossing wordt breder gezien dan de vraag. Samenwerking lijkt voor alle leveranciers mogelijk maar de invulling hiervan verschilt enorm. In de basis is de eigenaar van de informatie sturend in het al dan niet kunnen delen van informatie (departementaal samenwerken). De 'baseline' moet bij elk departement ingericht zijn. Onderzoek dient uit te wijzen welke extra facetten ingericht dienen te worden. Denk hierbij aan toegangscontrole, versleuteling data in transit, netwerk segmentatie, Zero trust beveiligingsmodel etc..



BEGIN MET WERKPROCES EN HOU HET KLEIN

4. Leveranciersperspectief

Inleiding

Service- en
implementatiemodel

Informatiebeveiliging

Implementatie

Additionele dienstverlening

6. Bent u in staat om de dienstverlening in te richten onder de voorwaarde dat deze alleen geleverd en uitgevoerd mag worden binnen de EER?

Het is voor geen van de leveranciers een probleem om de dienstverlening in te richten onder de voorwaarde dat deze alleen binnen een EER uitgevoerd mag worden.

Een van de partijen geeft wel aan dat nog nader uitgewerkt dient te worden.



TECHNOLOGISCH HEEFT DE MARKT VEEL MEER TE BIEDEN, MAAR DE IMPACT HIERVAN IS NIET ALTIJD DUIDELIJK

4. Leveranciersperspectief

Inleiding

Service- en
implementatiemodel

Informatiebeveiliging

Implementatie

**Additionele
dienstverlening**

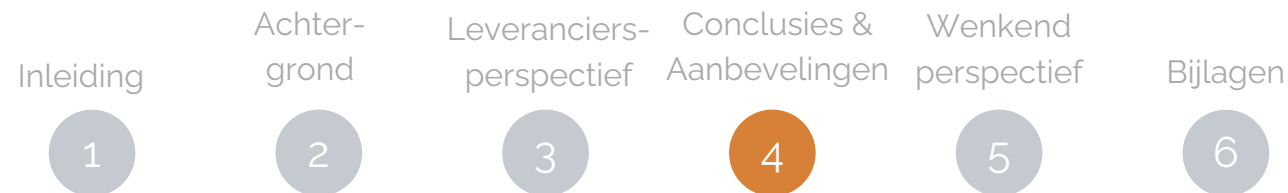
10. Gegeven de gehele vragen-set (hoofdstuk 3), welke additionele of complementaire diensten kunnen volgens u, vanuit uw kennis en ervaring met dergelijke trajecten en implementaties, ook interessant zijn voor de Vraagsteller? En waarom?

De antwoorden lopen uiteen van diensten met betrekking tot het ondersteunen van de proces- en organisatieveranderingen, het inbedden van verandermanagement en continu verbeteren tot aan meer technische oplossingen. Een leverancier stelt vooral randvoorwaarden.

Op basis van de aangeleverde antwoorden ligt de focus op het realiseren van een veilige, gebruiksvriendelijke, en flexibele content services omgeving met behulp van CSP, waarbij beveiliging een kernprioriteit is. Op de verschillende onderdelen worden diensten aangeboden door leveranciers.

4 Conclusies & Aanbevelingen

Wat zijn de belangrijkste conclusies die op basis van het onderzoek zijn vast te stellen? Welke aanbevelingen zijn er voor de departementen?



BEVEILIGINGSNIVEAU BBN₃ LIJKT NIET DIRECT EEN BEPERKING

6. Conclusies & Aanbevelingen

Conclusies - Antwoorden

Aanbevelingen

Kan de markt op basis van de beschikbare informatie een BBN₃ beveiligingsniveau leveren op de Rijkscloud?

Ondanks dat de markt inziet dat de invulling van de maatregelen behorend bij BBN₃ substantieel is, zien ze weinig tot geen problemen om dit op een voor lenW betrouwbare wijze dit in te richten. Hierbij worden verschillende oplossingen aangedragen. Over het hoe blijven de leveranciers vaag. Dan gaat het zowel om de rol van system integrator als de wijze waarop BBN 3 ketenbreed moet worden doorgevoerd. Samenwerking tussen verschillende departementen wordt als mogelijk gezien als hierbij aan voorwaarden voldaan wordt. De aard en inhoud van deze voorwaarden worden niet nader geduid.

In een aanbesteding zullen deze aspecten dan ook nader moeten worden uitgevraagd en beoordeeld op toereikendheid.

Ook het samenwerken op de Rijkscloud wordt, onder voorwaarden, als werkbaar geacht. Specifieke afspraken zijn nodig waardoor een 'SaaS' achtige dienstverlening voor lenW zeker een optie is. Richting en sturing vanuit lenW zijn hier essentieel.

BEVEILIGINGSNIVEAU BBN3 LIJKT NIET DIRECT EEN BEPERKING

6. Conclusies & Aanbevelingen

Conclusies - Antwoorden

Aanbevelingen

De specifieke uitwerking van de beveiligingseisen en de in te voeren maatregelen om hieraan te kunnen voldoen zijn essentieel voor een volledige en vergelijkbare aanbieding vanuit de leveranciers.

Het opstellen van heldere en functioneel goed omschreven voorwaarden met betrekking tot de eisen en maatregelen om te voldoen aan BBN3 lijken randvoorwaardelijk om een 'no bid' te voorkomen en meer dan 1 inschrijving te ontvangen. Daarbij is het belangrijk dat er inhoudelijke beoordeling plaats vindt van hoe de beveiliging ketenbreed wordt gerealiseerd. Dit betekent dat de BIO als eis gesteld moet worden, maar dat in een wens de maatregelen worden uitgewerkt.

5

Wenkend perspectief

Op basis van het onderzoek, en onze algemene ervaring en kennis, wordt een wenkend perspectief geschetst.

Inleiding

1

Achter-
grond

2

Leveranciers-
perspectief

3

Conclusies &
Aanbevelingen

4

Wenkend
perspectief

5

Bijlagen

6

I. BESTEED FUNCTIONEEL AAN, IN SAMENWERKING MET RIJKSCLOUD ALS CLOUD LEVERANCIER

5. Wenkend perspectief

Aanbesteding

Samenwerking

De markt geeft aan diensten op de Rijkscloud te kunnen leveren in combinatie met de beveiligingseisen BBN3. De voorwaarden die hieraan gesteld worden bieden een basis voor de uitvraag en maakt hiermee de weg vrij voor aanbesteden op de Rijkscloud.

IenW dient hiervoor helder te formuleren welke eisen van toepassing zijn en in welk model de dienst geleverd moet worden.

Vraag hierbij is:

- Een leverancier met onderaannemer(s)
- Meerdere leveranciers in een samenwerkingsverband
- Meerdere leveranciers met elk een eigen overeenkomst

Wenkend perspectief:

1. Definieer een aanbestedingsstrategie m.b.t. de service en implementatiemodellen.
2. Beoordeel de service integratie en implementatie op inhoud en maak hier een belangrijk onderdeel van de gunning van.
3. Hou in de business case rekening met extra kosten als de leverancier niet de volledige rol van service integratie op zich neemt.
4. Werk een visie uit m.b.t. het sturingsmodel



II. WERK HET OPTIMALE SERVICEMODEL UIT OP BASIS VAN DE BBN₃ VOORWAARDEN

5. Wenkend perspectief

Aanbesteding

Samenwerking

De markt geeft aan de gevraagde dienstverlening te kunnen leveren met randvoorwaarden. De aanbesteding dient de optimale vorm van samenwerking uit te vragen waarbij alle partijen optimaal kunnen bijdragen aan de gewenste functionaliteit en dienstverlening.

Wenkend perspectief:

1. Besteed in de aanbesteding veel aandacht aan het uitwerken van het optimaliseren van de samenwerking tussen partijen.
2. Beoordeel in de aanbesteding de voorgestelde maatregelen op kwaliteit en kijk daarbij ook naar de keten (koppelingen, generieke componenten waar de oplossing gebruik van maakt, et cetera)
3. Besteed specifieke aandacht bij de selectie van de technologische oplossingen en de implementatie aan benodigde afstemming tussen partijen (inclusief IenW).

III. ZET SAMENWERKING ALS THEMA IN DE AANBESTEDING

5. Wenkend perspectief

Aanbesteding

Samenwerking

De markt herkent de problematiek m.b.t. het departementaal samenwerken. De aanpak en technische invulling lijkt hiervoor sterk te verschillen tussen partijen. De verschillen gaan over inrichting, techniek en verantwoordelijkheden gebruikers.

IenW dient hiervoor helder te formuleren welke uitgangspunten van toepassing zijn bij de verwerving en inrichting van de oplossing.

Vragen hierbij zijn:

- Technische eisen m.b.t. tot toegang
- Functionele eisen m.b.t. samenwerking
- Awareness bij eindgebruikers m.b.t. compliancy (opleiding)

Wenkend perspectief:

1. Definieer een eenduidige set aan eisen specifiek voor samenwerking
2. Werk een visie uit m.b.t. het compliancy

6

Bijlagen

Inleiding

1

Achter-
grond

2

Leveranciers-
perspectief

3

Conclusies &
Aanbevelingen

4

Wenkend
perspectief

5

Bijlagen

6



AFKORTINGENLIJST

7. Bijlagen

Afkortingenlijst

Definities

Antwoorden Leveranciers

Verantwoording

BBN	-	Basisbeveiligingsniveau
CSP	-	Content Services Platform
DMS	-	Document Management Systeem
DMS-RMA	-	Document Management Systeem-Records Management Applicatie
IHH	-	Informatiehuishouding
FaaS	-	Function as a Service
IaaS	-	Infrastructure as a Service
PaaS	-	Platform as a Service
MDTO	-	Metagegevens voor duurzaam toegankelijke overheidsinformatie
RMA	-	Records Management Applicatie
SaaS	-	Software as a Service



DEFINITIES

7. Bijlagen

Afkortingenlijst

Definities

Antwoorden Leveranciers

Verantwoording

Content

Content is informatie met een betekenis gericht op een eindgebruiker of ontvanger van de content

Content Services Platform

Content Services Platforms (CSPs) zijn geïntegreerde platforms die content-gerichte diensten, repositories, API's, oplossingen en business processing tools aanbieden (Gartner).

Document management

Een centrale omgeving waarin documenten worden gecreëerd, opgeslagen, beheerd en geraadpleegd op basis van geautoriseerde toegang. Het gebruik is traceerbaar met audit trails en versiebeheer, waarmee wordt voldaan aan overheidsrichtlijnen ten aanzien van documentbeheer.

Records management

Recordsmanagement borgt dat informatie duurzaam en toegankelijk beheerd kan worden en dat wordt voldaan aan vigerende wet- en regelgeving

Informatie

Gegevens (data) die in een context (verband) zijn geplaatst en daardoor betekenis hebben gekregen in de vorm van text, spreadsheet, beeld, geluid, bericht (SMS, Social media) of ander voor gebruikers relevant elektronisch format.

Integratie processystemen

Het bouwblok Integratie processystemen borgt dat relevante informatie die in andere systemen wordt ontvangen of gecreëerd juist wordt opgeslagen en beheerd, optioneel binnen Document management en verplicht binnen Records management. Voor het werken met documenten kan ook aangesloten worden op het bouwblok Samenwerken intern en extern.

Samenwerken intern en extern

Samenwerken geeft invulling aan het intern en extern samenwerken aan documenten/content.

DEFINITIE DM(S)

7. Bijlagen

Afkortingenlijst

Definities

Antwoorden Leveranciers

Verantwoording

Een geautomatiseerd systeem dat de overheid in staat stelt digitale informatie (gegevens, records of digitale formulieren) ordentelijk op te slaan, te zoeken en te archiveren is, waarbij aan alle huidige (van toepassing zijnde) wet en regelgeving voldaan wordt. Het systeem moet alleen of in combinatie met andere systemen zaakgericht werken ondersteunen. Om ook toekomst vast te zijn dient het systeem bij wijzigende wet en regelgeving mee te kunnen bewegen door aangepaste inrichting (ondersteund door leverancier) of upgrades geleverd door leverancier.

1. Betrouwbare informatie

Betrouwbare informatie is de basis voor de taken en de sturing. De departementen maken onderscheid naar informatievoorziening ten behoeve van managementinformatie, die gebruikt wordt voor sturing en verantwoording, en de informatievoorziening die verweven is met het operationele proces.

2. Gestructureerde ondersteuning

Het systeem geeft inrichting aan generieke functionaliteit en waar mogelijk services voor de benoemde architectuur bouwblokken Post verwerking, Document management, Records management, E-mail integratie, Integratie processystemen, Samenwerken intern en extern en Zaakgericht werken / werkstroom

3. Duurzaam toegankelijk

Content moet voldoen aan de eisen voor de duurzame toegankelijkheid van overheidsinformatie volgens het Normenkader Duurzaam Toegankelijke Overheidsinformatie (DUTO).

4. Archiefwaardig

De bewaartermijnen van archiefwaardige content moet expliciet bewaakt worden. Door archiefwaardige content op één plaats beschikbaar te hebben zijn ze breed toegankelijk en kunnen bewaartermijnen worden gegarandeerd.



ANTWOORDEN LEVERANCIERS

7. Bijlagen

Afkortingenlijst

Definities

Antwoorden Leveranciers

Verantwoording

In de volgende slides is een samenvatting opgenomen van de antwoorden zoals gegeven door de leveranciers.

#	Vraag	Sub	Leverancier 1	Leverancier 2	Leverancier 3	Leverancier 4
1	1. Is uw oplossing in te richten op het implementatiemodel Rijkscloud en wordt hiermee de garantie gegeven dat de oplossing nu en in de toekomst door leverancier actueel gehouden wordt?	Implementatiemodel Rijkscloud	✓	✓	✓	✓
		Toekomstvast	✓	✓	✓	Leveriansmodel wordt nog onderzocht ✓
2	2. Kan de oplossing in samenwerking met Rijkscloud in een, voor het ministerie complementaire dienstverlening, als ware het een voor lenW SaaS dienstverlening aangeboden worden	SaaS vorm	✓	✓	✓	✓
						Afstemmen leveringsvoorwaarden partijen
3	3. Bent u bereid, gegeven de leveringsvoorwaarden van ODC Noord, om een continue dienstverlening te garanderen voor de gevraagde oplossing conform vraag 2?	Continue dienstverlening	✓	✓	✓	✓ Opstellen nadere afspraken ODC-Noord
4	4. Welke servicemodellen zijn er mogelijk op het implementatiemodel Rijkscloud als standaard dienstverlening?		Cafetariamodel op applicatie niveau Continuiteit en beschikbaarheid data Applicatielifecycle management Monitoring	IaaS PaaS SaaS FaaS	Managed Services Optimize Assist Program	Applicatie dienst Managed Services
5	5. Welke dienstverlening is er mogelijk op het implementatiemodel Rijkscloud?		Strategisch/Business consultancy Functioneel consultancy Technisch consultancy Development consultancy	Consultancy Support en Service Level Agreement Managed Services	Strategy & Advisory Services Consulting Services Learning Services Managed Services	Nader te bespreken Dienstverleningsmodel wordt intern uitgewerkt
6	6. Bent u in staat om de dienstverlening in te richten onder de voorwaarde dat deze alleen geleverd en uitgevoerd mag worden binnen de EER?		✓	✓	✓	✓ Model wordt nog nader uitgewerkt
7	7. Kunt u referenties aandragen waarbij u te maken heeft met BBN3 (of vergelijkbaar) in de Europese publieke sector en kunt u daarbij aangeven welke service-implementatiemodellen daarop van toepassing zijn?		Niet in deze fase Meerdere klanten binnen EER	--	Autoriteit persoonsgegevens, European central bank, NATO, Europese comissie (alles is geclassificeerd)	Defensie



ANTWOORDEN LEVERANCIERS

7. Bijlagen

Afkortingenlijst

Definities

Antwoorden Leveranciers

Verantwoording

#	Vraag	Sub	Leverancier 1	Leverancier 2	Leverancier 3	Leverancier 4
8	8. Wat is uw visie en aanpak m.b.t. BBN3 (of vergelijkbaar) in relatie met de geboden oplossing en gewenste dienstverlening?		Oplossing voldoet en kan meebewegen. Privacy by design (vanuit AVG/GDPR) Balans zoeken tussen algemeen belang en de werkbaarheid van een systeem	Visie gaat over:Beveiliging, Gebruiksvriendelijkheid, Flexibiliteit en schaalbaarheid Aanpak: Veilige gegevensopslag, Secure Access, Beveiligde gegevensoverdracht, Monitoring en auditing, Incidentrespons, Referentie Beveiligings-niveau Service-Compliance en regelgeving, Training en bewustwording, Interdepartementale samenwerking, Data Classificatie, Continu verbeteren.	Vanuit de oplossing en ons organisatie framework bieden we de middelen om aan BBN3 te kunnen voldoen. De invulling wordt gedaan samen met de proceseigenaren gebaseerd op risicomanagement. Aanpak: -Uitvoeren Risicoanalyse -Bepalen Classificatie van informatie -Opstellen Beleid en procedures a.d.h.v. beveiligings-eisen -Implementeren toegangscontrolemechanismen -Versleutelen gevoelige gegevens -Inrichten patch- en kwetsbaarhedenbeheer -Inrichten monitoring en logging -Trainen medewerkers security awareness -Opstellen Incident response plan -Uitvoeren Audits en compliance beoordelingen	Technisch kan BBN3 geïmplementeerd worden in onze oplossing. De implementatie van het service model vergt nog verdere afstemming.
9	9. Indien uw oplossing de mogelijkheid tot samenwerking tussen departementen in combinatie met het beveiligingsniveau BBN3 biedt, kun u aangeven aan welke voorwaarden voldaan moet worden?		Afhankelijk van acceptabele risico's en samenwerking departementen. Informatie tussen departementen wordt afgeschermd. Technisch afdoende mogelijkheden.	Aanvullende Overwegingen Versleuteling van End-to-End Communicatie: Rolgebaseerde Toegangscontrole: Geavanceerde Bedreigingsdetectie: Netwerksegmentatie: Disaster Recovery Plan: Patchbeheer: Zero Trust beveiligingsmodel: Juridische en Regulatieve Compliance: Implementatie in de organisatie - Cross-Functionele Teams: Management Ondersteuning	BBN3 in ieder geval binnen elk departement ingericht (baseline). Opstellen samenwerkingsplan (stappenplan vraag 8) Extra eis: eigenaar vaststellen en mandaad samenwerking (met name beveiliging 'data in transit')	Anonieme en ongeautoriseerde toegang tot informatie is niet mogelijk. Toegang moet geregeld zijn tot: de omgeving waarin het systeem draait; het platform zelf; het platform component (de content repository, zaak of het proces); de folder of samenwerkingsruimte; het document en de metadata. Aanvullende maatregelen met behulp van markeringen. Zorgen ervoor dat iemand expliciete toegang nodig heeft. Ook zijn er rolgebaseerde- of permanente lakmogelijkheden om informatie en metadata van een document te maskeren. Dit dient door len onderhouden te worden en vereist een koppeling met de directory service en een gedetailleerd beveiligingsplan.
10	10. Gegeven de gehele vragenset (hoofdstuk 3), welke additionele of complementaire diensten kunnen volgens u, vanuit uw kennis en ervaring met dergelijke trajecten en implementaties, ook interessant zijn voor de Vraagsteller? En waarom?		Leverancier biedt oplossingen voor organisaties op het gebied van digitale transformatie en informatiemanagement. Deze omvatten naast onze implementaties bij de Nederlands overheid ook een veelvoud aan implementaties in het bedrijfsleven. Leverancier raadt de Vraagsteller aan om niet alleen een focus op de trends in de overheidssector te hebben maar met een brede blik te kijken naar de mogelijke oplossingen en leveranciers.	Leverancier gaat graag het gesprek aan om te achterhalen wat de exacte behoeften van lenW zijn en hoe wij hen kunnen ondersteunen met de inzet van een nieuw Content Services Platform.	Vraagsteller zou er goed aan doen om expliciet te eisen dat beantwoording enkel gebaseerd mag zijn op door de vendor ontwikkelde producten / IP accelerators (reeds ontwikkelde diensten waar IP op berust). Indien mogelijk zal vraagsteller er goed aan doen om expliciet te stellen dat enkel het DigiGov Framework en Case Foundation Framework ontwikkeld door Leverancier Professional Services als basis mag worden gebruikt	Een van de technische oplossingsrichtingen is het inrichten volgens Zero Trust principe.



VERANTWOORDING LEVERANCIER ANALYSE

7. Bijlagen

Afkortingenlijst

Definities

Antwoorden Leveranciers

Verantwoording

Leveranciers

Op basis van de door IenW gedefinieerde extra vragen heeft QA Consultancy met behulp van het systeem iSourcingHub met behulp van dezelfde selectie van het voorgaande marktonderzoek dezelfde leveranciers benaderd. Deze lijst is besproken met de werkgroep en akkoord bevonden. Alle partijen zijn via iSourcingHub uitgenodigd om deel te nemen aan het extra marktonderzoek. Alle partijen zijn m.b.v. iSourcingHub actief benaderd.

Van de 19 partijen hebben er drie aangegeven niet te kunnen/willen meedoen. 11 partijen hebben niet gereageerd en 1 partij heeft na een initiële reactie alsnog niet gereageerd met een beantwoording.

De overgebleven vier leveranciers die wel hebben ingeschreven zijn:

1. OpenText
2. IBM
3. DocsPro
4. Delaware

De antwoorden van deze leveranciers zijn geanonimiseerd in dit rapport opgenomen en daarbij van een overkoepelende samenvatting voorzien. Daarbij is aangegeven of alle leveranciers (lees de markt), een deel van de leveranciers of enkele leveranciers een bepaalde mening waren toegedaan. Daar waar leveranciers geen of geen toepasselijk antwoord hebben gegeven, is dit in de tabellen aangegeven. "Geen toepasselijk antwoord" duidt op dat de vraag in die gevallen verkeerd is begrepen.

Het anonimiseren is bedoeld om het speelveld in een aanbesteding gelijk te houden en te voorkomen dat bepaalde partijen meer kennis of invloed hebben op een eventuele aanbesteding. Dit is in lijn met de regels voor een Marktonderzoek zoals beschreven op PIANOO.