



Ministerie van Infrastructuur
en Waterstaat

Bijlage 1 - Programma van Eisen

Aanbesteding Content Services Platform IenW

Versie	1.0
Datum	4 april 2024
Status	Definitief

INHOUD

1	Inleiding	3
1.1	Doel van het document	3
1.2	Structuur van dit document.....	3
2	Specificatie van eisen	4
3	Functionaliteit Content Services Platform	5
3.1	Diensten voor informatieobjecten	5
3.2	Diensten gericht op archivering.....	7
3.3	Diensten gericht op werkstromen	10
3.4	Diensten gericht op verzamelen van informatie	13
3.5	Diensten gericht op beschikbaar stellen informatie.....	14
3.6	Losse informatiediensten	16
3.7	Overstijgende diensten.....	18
3.8	Ondersteunende diensten	19
4	Technische eisen	23
4.1	Service Oriented Architecture	23
4.2	Standaarden Forum Standaardisatie	23
5	Informatiebeveiliging eisen	25
5.1	Actuele wetten en voorschriften	25
5.2	CIS & ABDO Controls.....	25
5.3	MDR, Logging en monitoring	32
5.4	Toekomstige ontwikkelingen	32
5.5	Autorisatie	33
5.6	Diensten van derden.....	33
5.7	Omgevingen.....	33
5.8	Privacy supplementen	34
5.9	Controle op naleving en melding incidenten.....	34
6	Integratie-eisen	35
6.1	Netwerkttoegang	35
6.2	Koppelpunt informatie-uitwisseling	35
7	Non-functionele eisen	36
7.1	Prestatie-efficiëntie	36
7.2	Bruikbaarheid	36
8	Beheer Content Services Platform	38
8.1	Diensten voor beheer van omgevingen.....	38
8.2	Diensten voor servicedesk	39
8.3	Diensten voor beheer autorisaties	40
9	Onderhoud Content Services Platform	42
9.1	Diensten voor preventief onderhoud	42
9.2	Diensten voor correctief onderhoud	42
9.3	Diensten voor adaptief en perfectief onderhoud.....	43
10	Uitvoeringseisen.....	45

1 Inleiding

1.1 Doel van het document

Dit Programma van Eisen beschrijft de gevraagde functionaliteit van de dienstverlening van de CSP oplossing welke het Ministerie van Infrastructuur en Waterstaat (IenW) als Opdrachtgever afneemt van opdrachtnemer en de eisen die specifiek aan de functionaliteit ervan en in het algemeen (= niet-functionele eisen) gesteld worden.

1.2 Structuur van dit document

In de volgende hoofdstukken worden de eisen beschreven die opdrachtgever inhoudelijk aan de oplossing van opdrachtnemer stelt:

3. Functionaliteit Content Services Platform;
4. Technische eisen;
5. Informatiebeveiliging eisen;
6. Integratie-eisen;
7. Non-functionele eisen;
8. Beheer Content Services Platform;
9. Onderhoud Content Services Platform.
10. Uitvoeringseisen

N.B Opdrachtnemer/Inschrijver dient aan alle eisen uit dit Programma van Eisen (PvE) te kunnen voldoen. Het niet kunnen voldoen aan een eis betekent knock-out (K.O.) en zal de inschrijving terzijde worden gelegd (zie ook paragraaf 3.10 van het beschrijvend document).

2 Specificatie van eisen

De eisen zijn vanuit het perspectief van opdrachtgever beschreven. Opdrachtnemer is er vanuit zijn professionaliteit voor verantwoordelijk de oplossing zodanig in te richten en te leveren dat het beoogde eindresultaat van elke eis telkens wordt bereikt. Met andere woorden, het blijft de verantwoordelijkheid van opdrachtnemer om gedurende de duur van de overeenkomst aan de vraagstelling van opdrachtgever (dus het 'wat') te blijven voldoen, hetgeen inhoudt dat opdrachtnemer zo nodig wijzigingen dient door te voeren in de eerder gekozen invulling van de vraagstelling (dus het 'hoe'). Daarbij geldt dat een dergelijke wijziging voor rekening en risico van opdrachtnemer is, tenzij de wijziging direct voortvloeit uit een gewijzigde vraagstelling van opdrachtgever.

De ICT-markt kenmerkt zich door vele en snelle ontwikkelingen en ook het Rijk en daarbinnen opdrachtgever zijn onderhevig aan ontwikkelingen. Gedurende de looptijd van de overeenkomst behoudt opdrachtgever zich het recht voor om bepaalde eisen te wijzigen als gevolg van markt-, Rijksbrede en (inter)departementale ontwikkelingen en voortschrijdend inzicht. Aanpassing van de oplossing wordt in overleg met de opdrachtnemer opgepakt.

3 Functionaliteit Content Services Platform

3.1 Diensten voor informatieobjecten

Doel van de dienst

Borgen dat de informatie die een medewerker nodig heeft binnen het dagelijkse werk gecreëerd, (her)gebruikt, gedeeld en bewaard kan worden. Daarbij wordt vastlegging van benodigde metadata geborgd, aangesloten op vigerende wet- en regelgeving en voorgesorteerd op archiveren in diensten gericht op *Archivering*.

Omschrijving van de dienst

Een centrale omgeving waar informatieobjecten in kunnen worden opgeslagen, gebruikt, beheerd en geraadpleegd op basis van geautoriseerde toegang. Het gebruik is traceerbaar met audit-trails en versiebeheer waarmee kan worden voldaan aan wetgeving (AVG, Archiefwet, Woo, enzovoort) en overheidsrichtlijnen ten aanzien van het beheer van informatieobjecten.

Een informatieobject is hier een verzameling aan elkaar gerelateerde gegevens, met een eigen identiteit, die als eenheid wordt behandeld.

Onderkende diensten:

- Opslaan informatieobject
- Versiebeheer informatieobject
- Fixeren informatieobject
- Verwijderen informatieobject
- Weergeven informatieobject

Eisen:

Nr	Omschrijving
	<i>Opslaan informatieobject</i>
DVI-001	De oplossing biedt de mogelijkheid een informatieobject op te slaan vanuit zowel een interne als een externe locatie, dat wil zeggen binnen en buiten de eigen ICT-infrastructuur van Opdrachtgever.
DVI-002	De oplossing biedt de mogelijkheid een informatieobject op te slaan vanuit Microsoft 365.
DVI-003	De oplossing biedt de mogelijkheid e-mails en bijlagen direct op te slaan als informatieobject vanuit Microsoft Outlook.
DVI-004	De oplossing biedt de mogelijkheid reeds bekende gegevens (eigenschappen van het bestand) automatisch over te nemen in metadata bij het opslaan van het informatieobject.
DVI-005	De oplossing biedt de mogelijkheid metadata bij het informatieobject vast te leggen.
DVI-006	De oplossing biedt de mogelijkheid te integreren met een Quick Address Server (QAS) t.b.v. postcode data zoeken en verifiëren.
DVI-007	De oplossing biedt de mogelijkheid aanvullende metadata te herleiden uit vastgelegde metadata of te overerven. Bijvoorbeeld: archiefwaardering, beveiliging en/of openbaarheidsbeperkingen.

Nr	Omschrijving
	<i>Versiebeheer informatieobject</i>
DVI-008	De oplossing biedt de mogelijkheid een informatieobject online te bewerken.
DVI-009	De oplossing biedt de mogelijkheid een informatieobject direct in de bronapplicatie te bewerken (zonder aanvullende handelingen als vooraf uitschakelen).
DVI-010	De oplossing biedt de mogelijkheid een informatieobject simultaan te bewerken door meerdere personen tegelijkertijd. Het informatieobject mag dus niet geblokkeerd worden door één gebruiker.
DVI-011	De oplossing toont bij gelijktijdige bewerking wie aan het informatieobject werken.
DVI-012	De oplossing ondersteunt versiebeheer van informatieobjecten.
DVI-013	De oplossing biedt de mogelijkheid een oudere versie te promoveren tot de meest actuele versie met behoud van de tot dan toe meest actuele versie.
DVI-014	De oplossing biedt de mogelijkheid bij een informatieobject direct een nieuwe versie toe te voegen vanaf een externe locatie (Toevoegen nieuwe versie).
DVI-015	De oplossing biedt de mogelijkheid metadata bij een versie van het informatieobject te bewerken.
	<i>Fixeren informatieobject</i>
DVI-016	De oplossing biedt de mogelijkheid een informatieobject te fixeren. Bijvoorbeeld het fixeren van een dataset of document met bepaalde status. Fixeren betekent dat de inhoud van het informatieobject niet meer aangepast kan worden.
	<i>Verwijderen informatieobject</i>
DVI-017	De oplossing biedt de mogelijkheid een informatieobject inclusief metadata te verwijderen.
	<i>Weergeven informatieobject</i>
DVI-018	De oplossing biedt de mogelijkheid de inhoud van een informatieobject middels een viewer of de bronapplicatie te raadplegen zonder een nieuwe versie te creëren.
DVI-019	De oplossing biedt de mogelijkheid om de inhoud van de metadata van een (specifieke versie van het) informatieobject weer te geven.
DVI-020	De oplossing biedt de mogelijkheid informatieobjecten te tonen binnen een ordening (metadata) gebaseerd op meerdere hiërarchische niveaus.

3.2 Diensten gericht op archivering

Doel van de dienst

De diensten gericht op archivering verzorgen de functionaliteit rondom het duurzaam en toegankelijk archiveren van informatieobjecten gedurende de wettelijke bewaar- en/of vernietigingstermijn.

3.2.1 Opname en classificatie

Omschrijving van de dienst

Het kunnen opnemen en/of importeren van informatieobjecten waarbij de informatie met behulp van metadata aan hun bedrijfscontext is gekoppeld.

Eisen:

Nr	Omschrijving
	<i>Creatie, opname en import van informatieobjecten</i>
DGA-001	De oplossing maakt het opnemen van informatieobjecten en bijbehorende metadata voor de informatieobjecten mogelijk.
DGA-002	De oplossing neemt een samengesteld informatieobject (bijvoorbeeld e-mail met bijlagen of een instant message of een document met ingevoegde objecten) op als gekoppelde informatieobjecten of als een enkel samengesteld informatieobject.
DGA-003	De oplossing biedt de mogelijkheid om informatieobjecten met bijbehorende metadata in grote hoeveelheden tegelijk of individueel te importeren, waarbij de integriteit van de inhoud en de structuur van de informatieobjecten wordt gegarandeerd.
DGA-004	De oplossing ondersteunt het opnemen van beschrijvingen (metadata) van fysieke informatieobjecten die zich elders in een bewaarplaats bevinden.
	<i>Opname van metadata voor informatieobjecten</i>
DGA-005	De oplossing biedt de mogelijkheid het opnemen en onderhouden van metadata bij alle informatieobjecten te ondersteunen, volgens één of meerdere vooraf vastgestelde metadata-schema's.
DGA-006	De oplossing biedt de mogelijkheid, alleen of in combinatie met andere applicaties, de waarden van metadata aan de hand van vooraf vastgestelde schema's en/of syntactische standaarden te valideren.
DGA-007	De oplossing biedt de mogelijkheid naast informatieobjecten ook werkstroominformatie, zoals proces metadata en historie, vast te leggen. Dit wordt opgeslagen/ bijgehouden in de eventgeschiedenis.
	<i>Classificatie van informatieobjecten</i>
DGA-008	De oplossing biedt de mogelijkheid aan alle werkstroomtypen een bewaartermijn te koppelen, zodat voor alle informatieobjecten bij een werkstroomtype automatisch de bewaartermijn wordt vastgelegd.
DGA-009	De oplossing biedt de mogelijkheid een bewaartermijn toe te kennen aan informatieobjecten waar dat geautomatiseerd niet mogelijk is, zodat voor alle informatieobjecten een correcte bewaartermijn is vastgelegd.

Nr	Omschrijving
DGA-010	De oplossing biedt de mogelijkheid de door het systeem toegekende bewaartermijn te wijzigen, zodat de bewaartermijn van een informatieobject aansluit bij de situatie van dat moment.
DGA-011	De oplossing biedt de mogelijkheid indien een informatieobject een relatie heeft met meerdere aggregaties van informatieobjecten met elk een andere bewaartermijn, dan automatisch de langst lopende bewaartermijn te overerven.
DGA-012	De oplossing biedt de mogelijkheid de metadata door een gebruiker te laten controleren en indien nodig (in bulk) aan te passen.
DGA-013	De oplossing biedt de mogelijkheid informatieobjecten op verschillende hiërarchische niveaus te groeperen en deze structuur te exporteren.
DGA-014	De oplossing biedt de mogelijkheid een goedgekeurd classificatieschema voor bedrijfsactiviteiten (selectielijst) te beheren en te onderhouden.
DGA-015	De oplossing biedt de mogelijkheid veranderingen in de bedrijfscontext (organisatiestructuur) te documenteren waarbij deze door de tijd heen gekoppeld blijft aan de informatieobjecten (reconstructie van bedrijfscontext borgen).

3.2.2

*Bewaring en vernietiging**Omschrijving van de dienst*

Informatieobjecten moeten bewaard en toegankelijk blijven voor bevoegde gebruikers zolang dit om juridische, maatschappelijke, bedrijfsmatige en zakelijke redenen nodig is. Overeenkomstig geautoriseerde bevoegdheden voor vernietiging behoren informatieobjecten op gecontroleerde, systematische en controleerbare wijze te worden bewaard en vernietigd.

Eisen:

Nr	Omschrijving
BV-001	De oplossing is in staat een passende bewaar- en vernietigingstermijn toe te wijzen voor elk informatieobject en elke aggregatie van informatieobjecten en maakt het mogelijk dat deze bewaar- en vernietigingstermijnen waar nodig vanwege veranderende wettelijke of bedrijfseisen wordt aangepast.
BV-002	De oplossing is in staat op basis van externe bedrijfsregels een passende bewaar- en vernietigingstermijn toe te wijzen voor elk informatieobject en elke aggregatie van informatieobjecten.
BV-003	De oplossing bewaart belangrijke metadata, waaronder metadata die de bevoegdheid tot vernietiging documenteren, voor het informatieobject en/of de aggregatie na vernietiging van het informatieobject en/of de aggregatie.
BV-004	De oplossing slaat de status van het informatieobject (en de aggregatie van informatieobjecten) vanaf de datum van vernietiging van het informatieobject op als 'Gewist' of 'Overgedragen aan X'.

Nr	Omschrijving
BV-005	De oplossing biedt de mogelijkheid de vernietigingstermijn tijdelijk stop te zetten om te voorkomen dat informatieobjecten vernietigd worden (Uitstel van vernietiging).
BV-006	De oplossing brengt een rapport uit over de vernietigingsstatus en -activiteit als het vernietigen van informatieobjecten wordt uitgevoerd (Proces verbaal van vernietiging).
BV-007	De oplossing biedt de mogelijkheid te bewaren informatieobjecten samen met de bijbehorende metadata over te brengen naar een intern archief van de organisatie of naar een archiveringsdienst van een bevoegde derde (exporteren).
BV-008	De oplossing biedt de mogelijkheid automatisch informatieobjecten te markeren die voor vernietiging in aanmerking komen en deze te vernietigen zodra de bewaartermijnen ervan zijn verstreken en de informatieobjecten beoordeeld zijn door een bevoegde gebruiker.
BV-009	De oplossing biedt de mogelijkheid een selectie te maken voor het uitvoeren van een vernietigingshandeling op basis van beschikbare metadata.

3.2.3

*Integriteit en onderhoud**Omschrijving van de dienst*

Interacties met of wijzigingen aan de informatieobjecten vastleggen. Metadata die deze interacties en wijzigingen vastleggen behoren de naam van de verantwoordelijke gebruiker, een tijdstempel en details van elke wijziging te omvatten. De metadata behoren blijvend gekoppeld te zijn aan de informatieobjecten, voor zolang zij bestaan.

Eisen:

Nr	Omschrijving
	<i>Integriteit en beveiliging van informatieobjecten</i>
IO-001	De oplossing bewerkstelligt dat de inhoud van informatieobjecten onveranderlijk kan worden gemaakt of kan worden beschermd tegen onbevoegde wijziging.
IO-002	De oplossing biedt beheersinstrumenten voor het wijzigen en bewerken van metadata overeenkomstig door de organisatie bepaalde bedrijfsregels tijdens archivering.
IO-003	De oplossing biedt de mogelijkheid checksums of hashes te genereren, of andere mechanismen te implementeren om integriteitscontrole op bepaalde momenten te ondersteunen.
IO-004	De oplossing biedt de mogelijkheid een informatieobject te voorzien van een gekwalificeerde digitale handtekening.
IO-005	De oplossing biedt de mogelijkheid beveiligde overdracht van informatieobjecten te ondersteunen, met inbegrip van het versleutelen van informatieobjecten voor beveiligde overdracht, indien van toepassing.

Nr	Omschrijving
	<i>Opslag, rapportage en beheer van metadata</i>
IO-006	De oplossing bewerkstelligt dat de informatieobjecten en de bijbehorende metadata die door de applicatie worden beheerd blijvend en veilig worden opgeslagen en dat ze door de tijd toegankelijk en opvraagbaar blijven voor bevoegde gebruikers.
IO-007	De oplossing biedt de mogelijkheid rapporten te produceren over het opnemen, gebruik en de vernietiging van informatieobjecten.
IO-008	De oplossing biedt de mogelijkheid verslag te doen van de acties die worden uitgevoerd op informatieobjecten, door de oplossing zelf of door bevoegde gebruikers en beheerders.
IO-009	De oplossing biedt de mogelijkheid rapportages met betrekking tot uitgevoerde vervangingsacties te genereren.
IO-010	De oplossing biedt de mogelijkheid de resultaten van de rapportages historisch in te kunnen zien. Mutaties moeten hierbij inzichtelijk en herkenbaar zijn.
IO-011	De oplossing biedt de mogelijkheid goedgekeurde metadataprofielen of -schema's door de tijd te beheren, te onderhouden en/of koppelingen ernaartoe te realiseren.

3.3 Diensten gericht op werkstromen

Doel van de dienst

De werkstroomdiensten verzorgen de functionaliteit rondom werkstroom- en procesinrichting om de totstandkoming en herleidbaarheid van de informatieobjecten te begeleiden.

Omschrijving van de dienst

De dienst geleidt een medewerker door een werkstroom of proces en attendeert de gebruiker op foutieve of ontbrekende invoer of handelingen. Ook voorziet zij de medewerker van inzicht in status van de processen.

De dienst ondersteunt het gebruik van bedrijfsregels en overerving van procesmodellen als bron voor een proces gestuurde aanpak zoals een zaak (dossier). Een zaak is in dit verband een samenhangende hoeveelheid werk (taken), met een duidelijke aanleiding en een duidelijk resultaat. Het concept van in werkstromen werken legt een raamwerk van statusovergangen over de werkstromen of processen heen.

Ook elektronisch paraferen, elektronisch ondertekenen en afhandelen van Woo-verzoeken kunnen onder deze dienst beschouwd worden.

Onderkende diensten:

- Modelleren en inrichten van processen en werkstromen (procespatronen)
- Routeren informatieobject
- Dossieropbouw en dossiervorming
- Elektronisch paraferen en goedkeuringsprocessen
- Bewaken voortgang werkstroom
- Samenwerken

Eisen:

Nr	Omschrijving
	<i>Modelleren en inrichten van processen en werkstromen (procespatronen)</i>
DGW-001	De oplossing ondersteunt een visuele omgeving waarin processen gemodelleerd kunnen worden.
DGW-002	De oplossing biedt de mogelijkheid procestemplates in te richten, te configureren (bijvoorbeeld aan- en uitzetten standaardopties en inrichten metadata) en te kopiëren.
DGW-003	De oplossing ondersteunt gestructureerde (vaste volgorde processtappen) en ongestructureerde processen (gebruiker bepaalt volgorde processtappen).
DGW-004	De oplossing biedt de mogelijkheid op basis van business rules processtappen in te richten.
DGW-005	De oplossing biedt functionaliteit voor het in de tijd agenderen van taken (termijnbewaking).
DGW-006	De oplossing houdt informatie ter besturing en verantwoording rondom de afhandeling van processen bij.
DGW-007	De oplossing biedt de mogelijkheid functionele uitval te corrigeren. Bijvoorbeeld: corrigeren metadata, processtap opnieuw uitvoeren of terugzetten.
	<i>Routeren informatieobject</i>
DGW-008	De oplossing biedt de mogelijkheid generieke en specifieke metadata (behorend bij een type werkstroom) bij een werkstroom vast te leggen.
DGW-009	De oplossing biedt de mogelijkheid metadata bij een werkstroom aan te passen.
DGW-010	De oplossing biedt inzicht in openstaande processtappen (werkvoorraad). Deze overzichten zijn te splitsen naar rol of persoon.
DGW-011	De oplossing biedt de mogelijkheid processtappen naar gebruikers of gebruikersgroepen te routeren.
DGW-012	De oplossing biedt de mogelijkheid handmatig en parallel een geconfigureerde processtap te starten (bijvoorbeeld informeren, notificeren)
DGW-013	De oplossing biedt de mogelijkheid parallel een processtap te starten (bijvoorbeeld afstemmen).
DGW-014	De oplossing biedt de mogelijkheid met externe gebruikers (medewerkers buiten de organisatie) samen te kunnen werken aan informatieobjecten binnen een werkstroom.
	<i>Dossieropbouw en dossiervorming</i>
DGW-015	De oplossing biedt de mogelijkheid voor het tonen en bijwerken (toevoegen, verwijderen, bijwerken) van de bij een werkstroom horende informatieobjecten (dossier).

Nr	Omschrijving
DGW-016	De oplossing biedt de mogelijkheid voor het relateren van notities (opmerkingen) aan een proces.
DGW-017	De oplossing biedt de mogelijkheid binnen een werkstroom per onderwerp een dossier op te bouwen, zodat alle informatieobjecten bij elkaar staan en per onderwerp vindbaar zijn.
DGW-018	Een informatieobject moet meerdere keren gekoppeld en aan elkaar gerelateerd kunnen worden zodat een informatieobject deel uit kan maken van meerdere werkstromen en dossiers.
DGW-019	De oplossing biedt de mogelijkheid afzonderlijke werkstromen en bijbehorend dossier aan elkaar te relateren (bijvoorbeeld ingeval van bezwaar en beroep). Hierbij is overzicht in de hele procesketen beschikbaar.
DGW-020	De oplossing biedt de mogelijkheid dat zodra de laatste status is gezet, de behandelaar de werkstroom en bijbehorende informatieobjecten niet meer inhoudelijk kan wijzigen, toevoegen en verwijderen. Dit kan alleen nog door hiertoe geautoriseerde gebruikers en beheerders.
DGW-021	De oplossing biedt de mogelijkheid te signaleren dat bij het afsluiten van een werkstroom een bepaald type document (met de status "verplicht") uit het onderliggende werkproces ontbreekt.
DGW-022	De oplossing biedt de mogelijkheid te informeren bij het afsluiten van een werkstroom richting één of meerdere ontvangers.
	<i>Digitaal paraferen en goedkeuringsprocessen</i>
DGW-023	De oplossing biedt de mogelijkheid standaard paraferenroutes in te richten op basis van werkstroom in combinatie met functie gebruiker (bijvoorbeeld afdelingshoofd of directeur) en organisatieonderdeel.
DGW-024	De oplossing biedt de mogelijkheid een standaard goedkeuringsproces aan te passen bij een werkstroom.
DGW-025	De oplossing biedt de mogelijkheid het goedkeuren van informatieobjecten flexibel in te stellen, zodat bij afwezigheid het paraferen door collega's kan worden overgenomen.
DGW-026	De oplossing ondersteunt digitaal paraferen van informatieobjecten.
	<i>Bewaken voortgang werkstroom</i>
DGW-027	De oplossing houdt de status van de afhandeling van een werkstroom bij.
DGW-028	De oplossing biedt de mogelijkheid de uitvoering van werkstromen te monitoren. Bijvoorbeeld op doorlooptermijn, werkverdeling en status.
DGW-029	De oplossing biedt de mogelijkheid een termijn aan te passen binnen de werkstroom (inclusief uitstellen).
DGW-030	De oplossing biedt de mogelijkheid een termijn in een wachtstand te zetten ('stop de klok') binnen de werkstroom.

Nr	Omschrijving
DGW-031	De oplossing biedt de mogelijkheid medewerkers te notificeren bij het ontvangen van een processtap of afhandeling van een processtap.
DGW-032	De oplossing biedt de mogelijkheid een processtap over te nemen van een collega.
DGW-033	De oplossing biedt de mogelijkheid in te grijpen binnen een zaak, bijvoorbeeld een zaak toewijzen aan een andere behandelaar.
DGW-034	De oplossing biedt de mogelijkheid om uitval in te zien bij gestructureerde processen (bijvoorbeeld fouten bij uitvoeren processtappen, fouten bij een koppeling naar een gestructureerd proces, fouten bij archivering van een proces).
DGW-035	De oplossing biedt de mogelijkheid inzicht te bieden in de historie bij een werkstroom (uitgevoerde gebruikershandelingen – audit trail).
DGW-036	De oplossing biedt inzicht in de status van informatieobjecten (bijvoorbeeld opmerkingen, mutaties, voortgang van taken, termijnbewaking en dergelijke)
DGW-037	De oplossing biedt een dashboardfunctie waarmee de stand van zaken bij werkstromen ingezien kan worden (bijvoorbeeld status, doorlooptijd).
	Samenwerken
DGW-038	De oplossing biedt de mogelijkheid samen te werken aan informatieobjecten.
DGW-039	De oplossing biedt de mogelijkheid samen te werken met medewerkers binnen Opdrachtgever, binnen de Rijksoverheid en externe organisaties.
DGW-040	De oplossing biedt de mogelijkheid leden binnen de samenwerking te notificeren bij het verlopen van een ingestelde termijn.

3.4 Diensten gericht op verzamelen van informatie

Doel van de dienst

Diensten gericht op het vastleggen van informatieobjecten in de oplossing, die in de omgeving van de oplossing zijn ontstaan.

Omschrijving van de dienst

In de omgeving van de oplossing ontstaan informatieobjecten en zijn informatieobjecten aanwezig, bijvoorbeeld door het scannen van informatie op papier en informatieobjecten in andere systemen. Deze informatieobjecten dienen reactief (pull) dan wel proactief (push) opgenomen te kunnen worden in de oplossing.

Onderkende diensten:

- Ontvangen informatieobject
- Ophalen informatieobject

Eisen:

Nr	Omschrijving
	<i>Ontvangen informatieobject</i>
DGI-001	De oplossing biedt de mogelijkheid om informatieobjecten aangeboden van buiten de oplossing op te slaan, waarbij bekende gegevens automatisch als metadata worden opgeslagen en handmatig andere metadata kan worden aangevuld.
DGI-002	De oplossing biedt de mogelijkheid te integreren met gangbare scanoplossingen, waaronder Kofax.
DGI-003	De oplossing biedt de mogelijkheid om, indien het ontvangen informatieobject (gescande) post betreft, het postproces te ondersteunen en traceerbaar te maken.
DGI-004	De oplossing biedt de mogelijkheid om e-mails die ontvangen zijn in persoonlijke en groepsmailboxen op basis van diverse criteria te selecteren, op te halen en duurzaam toegankelijk op te slaan, waarbij bekende gegevens automatisch als metadata worden opgeslagen en handmatig andere metadata kan worden aangevuld.
	<i>Ophalen informatieobject</i>
DGI-005	De oplossing biedt de mogelijkheid om informatieobjecten op te halen vanuit andere systemen, zowel op basis van push als pull.

3.5 Diensten gericht op beschikbaar stellen informatie

Doel van de dienst

Het doel van de dienst is het intern opdrachtgever en extern beschikbaar stellen van informatie op basis van informatieobjecten aanwezig in de oplossing.

Omschrijving van de dienst

De informatieobjecten binnen de oplossing moeten beschikbaar worden gemaakt voor buiten de oplossing. Intern opdrachtgever betreft dat bijvoorbeeld het delen van een informatieobject met collega's en systemen, het publiceren op het intranet en het ontsluiten van de oplossing door de enterprise search engine oplossing van opdrachtgever. Extern opdrachtgever gaat het om bijvoorbeeld het aanbieden van een informatieobject ter publicatie.

Onderkende diensten:

- Ontsluiten informatieobject
- Publiceren informatieobject
- Migreren en exporteren informatieobject

Eisen:

Nr	Omschrijving
	<i>Ontsluiten informatieobject</i>
DGBI-001	De oplossing biedt de mogelijkheid informatieobjecten te zoeken op basis van metadata en full tekst door middel van een intuïtieve zoekfunctie (bijvoorbeeld eenvoudig zoeken met open zoekveld of veel voorkomende metadatavelden als <i>titel</i>).
DGBI-002	De oplossing biedt de mogelijkheid verder te filteren in zoekresultaten (facetstructuur).
DGBI-003	De oplossing biedt de mogelijkheid complexe zoekvragen op te slaan en te delen met andere gebruikers en beheerders.
DGBI-004	De oplossing biedt de mogelijkheid informatieobjecten op te halen en deze in een bruikbaar formaat weer te geven.
DGBI-005	De oplossing biedt de mogelijkheid één of meerdere informatieobjecten dan wel een link naar één of meerdere informatieobjecten in de oplossing veilig te delen met collega's tenminste via e-mail. In geval van een link kan het ook om een verzameling informatieobjecten (dossier) gaan.
DGBI-006	De oplossing biedt de mogelijkheid een via een link gedeeld informatieobject direct en eenvoudig te kunnen inzien en bewerken.
DGBI-007	De oplossing biedt de mogelijkheid informatieobjecten te delen met andere systemen, waarbij het informatieobject niet wordt verplaatst of gekopieerd naar die andere systemen.
DGBI-008	De oplossing biedt de mogelijkheid informatieobjecten door te geven aan andere systemen, waarbij het informatieobject wordt verplaatst of gekopieerd naar die andere systemen.
DGBI-009	De oplossing biedt de mogelijkheid dat de metadata en de inhoud van informatieobjecten kunnen worden ontsloten door de door Opdrachtgever gebruikte enterprise search oplossing Zoek en Vind.
	<i>Publiceren informatieobject</i>
DGBI-010	De oplossing biedt de mogelijkheid informatieobjecten intern te publiceren op een intranet. De oplossing dient bij te houden, dat het informatieobject intern gepubliceerd is.
DGBI-011	De oplossing biedt de mogelijkheid het proces van extern publiceren te ondersteunen door het geven van inzicht in extern te publiceren en gepubliceerde informatieobjecten en link naar de publicatie.
DGBI-012	De oplossing biedt de mogelijkheid om informatieobjecten aan te bieden aan een intern systeem ter voorbereiden van het publiceren op een platform ten behoeve van externe publicatie, waarbij de metadata beperkt is tot het voor externe publicatie benodigde minimum.
DGBI-013	De oplossing biedt de mogelijkheid om de status van extern gepubliceerde informatieobjecten te ontvangen van een systeem en op te slaan.

Nr	Omschrijving
	Converteren, migreren en exporteren informatieobject
DGBI-014	De oplossing biedt de mogelijkheid zoekresultaten (in bulk) te exporteren, het betreft export van informatieobjecten met bijbehorende metadata.
DGBI-015	De oplossing biedt de mogelijkheid informatieobjecten en bijbehorende metadata en, indien van toepassing, aggregaties van informatieobjecten te converteren/migreren/exporteren naar: - een geschikt of meer actueel gegevensbestandsformaat voor de informatieobjecten dat het voortdurend bewaren en gebruiken ervan ondersteunt; - een andere bedrijfsapplicatie binnen de opdrachtgeveromgeving van de opdrachtgever; - een vervangende bedrijfsapplicatie wanneer het tijd wordt de bronapplicatie buiten bedrijf te stellen; en/of - een systeem buiten de opdrachtgeveromgeving van de opdrachtgever.
DGBI-016	De oplossing biedt de mogelijkheid in alle migratie-/exportaties het volgende mee te nemen: - alle informatieobjecten en, waar van toepassing, aggregaties van informatieobjecten; - metadata voor de geschiedenis van gebeurtenissen in verband met geëxporteerde informatieobjecten (functionele audit trail).

3.6 Losse informatiediensten

Doel van de dienst

De losse informatiediensten zijn diensten die aangeroepen kunnen worden in/vanuit de oplossing voor het invullen van specifieke aanvullende functies binnen het informatielandschap.

Omschrijving van de dienst

Onderkende losse informatiediensten zijn:

- Aanmaken informatieobject met als specialisatie: Genereren document
- Anonimiseren informatieobject met als specialisatie: Lakken informatie
- Converteren informatieobject
- Digitale handtekening
- Enterprise search
- Genereren document
- Paraferen document
- Pseudonimiseren informatieobject
- Zwartlakken informatie

Onderstaand zijn de losse diensten beschreven met daarbij aangegeven of met deze dienst geïntegreerd dient te worden of dat deze dienst door de oplossing gerealiseerd dient te worden.

Aanmaken informatieobject

Dienst voor het aanmaken van een informatieobject op basis van metadata en eventueel een sjabloon. Op dit moment ondersteunt door de oplossing DocGen, als dienst afgenomen van Doc-Direkt.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Anonimiseren informatieobject

Dienst om uit een informatieobject gegevens te verwijderen die naar een (rechts)persoon herleidbaar kunnen zijn. Het resultaat van een geanonimiseerd informatieobject is een nieuw informatieobject. De relatie tussen het oude en nieuwe object wordt bij de beide objecten vastgelegd. Nog geen oplossing voor beschikbaar.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Converteren informatieobject

Dienst voor het omzetten van informatieobjecten in een ander dataopslagformaat. N.B.: Uitgangspunt is dat informatieobjecten niet onnodig worden omgezet. Nog geen oplossing voor beschikbaar.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Digitale handtekening

Dienst Digitaal Ondertekenen Informatieobject, ook bekend als digitale handtekening, is een dienst voor het garanderen van de juistheid van digitale informatie die zowel intern als extern beschikbaar is. De dienst bestaat uit drie onderdelen: 1) methode om te garanderen dat de informatie niet gewijzigd is (onweerlegbaarheid), 2) de identiteit van de ondertekenaar te bevestigen (identiteit) en 3) de authenticiteit van het informatieobject te borgen. Op dit moment ondersteunt door de oplossing eHandtekening, als dienst afgenomen van Doc-Direkt.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Enterprise search

Een IenW brede zoekfunctionaliteit door alle bronsystemen waarin informatieobjecten zijn opgeslagen. Op dit moment ondersteunt door de oplossing Zoek en Vind, als dienst afgenomen van Doc-Direkt.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Genereren document

Het creëren van een document op basis van een vooraf gedefinieerd sjabloon, content en/of aangeleverde metadata. Dit is meestal aan het begin van een proces of aan het einde van een proces. Dit is afhankelijk van het type proces. Op dit moment ondersteunt door de oplossing DocGen, als dienst afgenomen van Doc-Direkt.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Paraferen document

Dienst die kan worden aangeroepen om documenten te paraferen. Andere weergaven van informatieobjecten worden niet geparafeerd. Op dit moment ondersteunt door de oplossing eParaferen, als oplossing door opdrachtgever gerealiseerd.

➔ Deze dienst wordt door de oplossing gerealiseerd.

Pseudonimiseren informatieobject

Dienst voor het vervangen van identificerende gegevens door versleutelde gegevens (het pseudoniem). Hierbij wordt voor een (rechts)persoon altijd hetzelfde pseudoniem gebruikt, waardoor informatie over de (rechts)persoon, kan worden gerelateerd.

Het gepseudonimiseerde informatieobject is een nieuw informatieobject. De relatie tussen het oude en nieuwe object wordt bij de beide objecten vastgelegd. Nog geen oplossing voor beschikbaar.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Zwartlakken informatie

Een dienst die in het verlengde ligt van anonimiseren. In dit geval worden ook andere kenmerken vervangen door zwarte balken. Op dit moment ondersteunt door de oplossing Zylab.

➔ Deze dienst wordt geïntegreerd met de oplossing.

Eisen:

Nr	Omschrijving
LI-001	De oplossing stelt het paraferen van informatieobjecten als dienst beschikbaar aan andere diensten binnen het systeemlandschap van opdrachtnemer.
LI-002	De oplossing biedt de mogelijkheid om te integreren met de eHandtekening oplossing.
LI-003	De oplossing biedt de mogelijkheid om te integreren met de iBabs oplossing.
LI-004	De oplossing biedt de mogelijkheid om informatieobjecten en metadata door de Enterprise search oplossing (Zoek en Vind) te laten indexeren (doorzoekbaar te maken).
LI-005	De oplossing biedt de mogelijkheid een nieuw gerelateerd informatieobject op te slaan na deze te hebben ontvangen na het aanroepen van de diensten: - Anonimiseren informatieobject - Converteren informatieobject - Digitale handtekening - Genereren document - Paraferen document - Pseudonimiseren document. - Zwartlakken informatie
LI-006	De oplossing biedt de mogelijkheid om een nieuw informatieobject op te slaan na het aanroepen van de dienst Genereren document of Aanmaken informatieobject.
LI-007	De oplossing biedt de mogelijkheid om te integreren met de DocGen oplossing.

3.7 Overstijgende diensten

Doel van de dienst

Het beveiligen van het informatie(object) en het beheren van metadata zijn overstijgende diensten, waarbij delen van de diensten door de oplossing worden ingevuld.

Omschrijving van de dienst

Het beveiligen van een informatieobject is de verantwoordelijkheid van het bronsysteem eventueel aangevuld door de archiveringsdiensten. Echter indien een informatieobject als een kopie wordt opgeslagen dient de oplossing voor het nieuwe informatieobject de rechten af te leiden van het oorspronkelijk informatieobject.

- ➔ Deze dienst wordt door de oplossing ingevuld eventueel in samenwerking met andere overstijgende diensten.

Metadata voor de informatieobjecten worden beheerd in de systemen waarin de informatieobjecten zijn opgeslagen, de bronsystemen, en de systemen die de archiveringsdiensten realiseren. Zij bepalen welke metadata opslagen kunnen worden. Als een aanvullende dienst noodzaak heeft aan niet ondersteunde metadata dan is deze dienst zelf verantwoordelijk voor de opslag en het beheer van deze gegevens.

Metadata Duurzaam Toegankelijke Overheidsinformatie (MDTO) vervangt de huidige afgesproken standaard: Toepassingsprofiel Metadata Rijksoverheid (TMR). Hiervoor geldt een overgangperiode van 3 jaar. In een vervolgtraject worden nadere detailleringen uitgewerkt, waaronder metadata over bedrijfsactiviteiten, actoren en mandaten (wat, waar en door wie) gestandaardiseerd. In de overgangperiode mogen binnen de Rijksoverheid zowel MDTO als TMR gebruikt worden.

- ➔ Deze dienst wordt door de oplossing ingevuld eventueel in samenwerking met andere overstijgende diensten.

Eisen:

Nr	Omschrijving
	<i>Beveiligen informatie</i>
OD-001	De oplossing biedt de mogelijkheid de beveiliging van een informatieobject aan te leveren aan een ander systeem.
OD-002	De beveiliging van het informatieobject gebeurt middel RBAC (Role Based Access Control) en ABAC (Attribute Based Access Control).
	<i>Beheren metadata</i>
OD-003	De oplossing biedt ondersteuning van MDTO bij opslag van informatieobjecten.
OD-004	De oplossing biedt ondersteuning van TMR bij opslag van informatieobjecten.
OD-005	De oplossing biedt ondersteuning van MDTO bij het uitwisselen van informatie(objecten).
OD-006	De oplossing biedt de mogelijkheid om metadata op te slaan en te beheren buiten het bronsysteem.

3.8 Ondersteunende diensten

Doel van de dienst

De ondersteunende diensten zijn geen onderdeel van de oplossing, maar zijn wel van cruciaal belang, sommige randvoorwaardelijk, voor het gebruik van de oplossing. Dit zijn de werkplekdiensten, monitoren, datadiensten en logbeheer. De oplossing ondersteunt deze diensten.

3.8.1 Werkplekdiensten

Omschrijving van de dienst

Werkplekdiensten bieden de gebruikers toegang tot de informatie(systemen) en maken het mogelijk om informatieobjecten te bewerken.

Onderdeel van deze dienst kan zijn het gelijktijdig bewerken van informatieobjecten. Hiermee wordt het mogelijk voor verschillende gebruikers om gelijktijdig in een document te werken en de bewerkingen van anderen te zien terwijl deze plaatsvinden. De bijgewerkte versies worden in het bronsysteem opgeslagen.

Deze dienst wordt ook ingevuld door werkplekdiensten door gebruik te maken van IHH-dienst *Bewerken informatieobject* (zie ook eisen paragraaf 3.1). Deze zorgt voor het ophalen van het informatieobject.

Weergeven informatieobject (zie ook eisen paragraaf 3.1) zorgt voor het ophalen van het informatieobject. Waar de invulling binnen de informatieobject diensten zich richt op gangbare bestandsformaten, kan de invulling binnen de werkplekdiensten zich ook richten op minder gangbare bestandsformaten die met specifieke werkplekapplicaties getoond dienen te worden.

Eisen:

Nr	Omschrijving
WD-001	De oplossing biedt de mogelijkheid om te integreren met Microsoft 365.
WD-002	De oplossing biedt de keuze om de werkplekapplicatie te gebruiken voor het weergeven van informatieobjecten.
WD-003	De oplossing ondersteunt de werkplekapplicaties door middel van services voor het opvragen en opslaan van (versies) van informatieobjecten.
WD-004	De oplossing draait op de 3 meest recente versies van de top 5 browsers (Edge, Chrome, FireFox, Safari, Opera).
WD-005	De oplossing is met een tablet en/of smartphone (Android of IOS) benaderbaar en functioneert en correct (volledige responsiveness). - Tablet Android - Smartphone Android - Tablet IOS (iPad) - Smartphone IOS (iPhone)
WD-006	De oplossing is benaderbaar binnen Blackberry UEM client (tot twee versies terug).
WD-007	Buiten een browser en de integratie met Microsoft 365 mag er geen andere afhankelijkheid van de werkplek zijn, met andere woorden de updates van de werkplek mogen geen invloed hebben op de werking van de oplossing.

3.8.2 Monitoring

Omschrijving van de dienst

De losse componenten binnen het huidige applicatielandschap van opdrachtgever creëren een lappendeken aan diensten. Een algehele monitoringdienst maakt het mogelijk hier overzicht en inzicht in te krijgen. Elke component is verantwoordelijk voor het beschikbaar stellen van de logginginformatie aan deze monitoringdienst. Naast het aansluiten op de centrale monitoringdienst biedt de oplossing ook een eigen monitoringfunctionaliteit.

Eisen:

Nr	Omschrijving
MT-001	De oplossing biedt monitoringfunctionaliteit voor het monitoren van alle onderdelen van de oplossing en het voortbrengingsproces van de oplossing.
MT-002	De oplossing biedt de mogelijkheid vastgelegde logging informatie aan te leveren aan een centrale monitoringsdienst.

3.8.3 Logbeheer

Omschrijving van de dienst

Centrale plaats waar alle relevante loggegevens worden verzameld en geanalyseerd.

Eisen:

Nr	Omschrijving
LB-001	De oplossing biedt alle relevante logging aan, aan een centraal punt waar de logging geanalyseerd kan worden.
LB-002	De oplossing biedt de mogelijkheid technische logging vast te leggen, het gaat hierbij om informatie om te bepalen of de oplossing correct wordt gebruikt.
LB-003	De oplossing biedt de mogelijkheid algemene logging vast te leggen, het gaat hierbij o.a. om informatie rondom toegang tot en raadpleging van informatieobjecten.
LB-004	De oplossing biedt de mogelijkheid auditlogging vast te leggen, het gaat hierbij om handelingen op het niveau van informatieobjecten, dossiers en processen.
LB-005	De oplossing biedt de mogelijkheid auditlogging vast te leggen van beheerhandelingen.

3.8.4 Datadiensten

Omschrijving van de dienst

Centrale ingang voor diensten rondom data-analyse en rapportages over de IHH-diensten en het gebruik. Deze worden inzichtelijk gemaakt via dashboards zoals de dashboards voor IHH-kenmerken.

Eisen:

Nr	Omschrijving
DAD-001	De oplossing biedt de mogelijkheid via een mechanisme alle metadata van alle informatieobjecten beschikbaar te stellen aan de datadiensten voor rapportages.
DAD-002	De oplossing biedt de mogelijkheid op basis van type informatieobject, aanmaakmoment of bijwerkmoment alle metadata van informatieobjecten beschikbaar te stellen aan de datadiensten voor rapportages.
DAD-003	De oplossing biedt de mogelijkheid dagelijks alle metadata van alle nieuw aangemaakte of aangepaste informatieobjecten beschikbaar te stellen aan de datadiensten voor rapportages.
DAD-004	De oplossing biedt de mogelijkheid werkstroomdata en logging beschikbaar te stellen aan de datadiensten voor rapportages.

3.8.5 *IAM (Identity and Access Management)*

Omschrijving van de dienst

Gebruik van de SSO's¹ Rijk voorziening faciliteert het authenticeren van gebruikers bij het toegang verkrijgen tot de diensten. Momenteel is SAML nog de enige optie, daar komt in de toekomst OpenID-Connect bij. Totdat OpenID-Connect beschikbaar is, zal het systeem SAML moeten ondersteunen. Daarna zal het systeem OpenID-Connect moeten ondersteunen.

Eisen:

Nr	Omschrijving
IAM-001	De oplossing gebruikt SSO's Rijk, op basis van SAML en OpenID-Connect, voor het authenticeren van gebruikers.
IAM-002	De oplossing biedt een autorisatiemechanisme met daarin een eigen functie voor het beheren van groepen en gebruikers.
IAM-003	De oplossing maakt gebruik van SCIM voor het ophalen van gebruikersgegevens.
IAM-004	De oplossing houdt door middel van een audit trail mutaties aan gebruikers en groepen binnen de oplossing bij en deze blijven conform vastgestelde bewaartermijn beschikbaar.
IAM-005	Elke gebruiker en groep heeft een uniek intern kenmerk.
IAM-006	De rechten die beheerders hebben binnen de oplossing zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.

¹ SSO = Single Sign On

4 Technische eisen

4.1 Service Oriented Architecture

Toelichting

De beschreven architectuur is opgebouwd uit verschillende diensten die technisch ingevuld worden door services. Onze voorkeur is dat elke service uit één of meerdere losstaande microservices bestaat. Alleen als er aantoonbare meerwaarde is voor beheersbaarheid of kwaliteit kan hiervan worden afgeweken.

Voor elke service wordt afzonderlijk bepaald welke onderliggende techniek binnen de gestelde kaders het beste past.

De microservices zijn modulair waarbij geldt dat elke service een aanvulling is op de andere microservices. Daarbij worden de microservices autonoom ontwikkeld en beheerd zonder technische afhankelijkheden van andere services. Elke microservice is daarom *state less* en, indien microservice gebruik maakt van een andere service die tijdelijk offline is, mag de microservice niet voor fouten zorgen.

De microservices zijn geautomatiseerd schaalbaar waarbij vooraf kan worden aangegeven wanneer en hoe de services opgeschaald worden.

Eisen:

Nr	Omschrijving
TES-001	De aangeboden oplossing bestaat uit losse services.

4.2 Standaarden Forum Standaardisatie

Toelichting

Alle technische voorzieningen van de oplossing moeten voldoen aan de onderstaande lijst standaarden (en opvolgers) van het Forum Standaardisatie.

Eisen:

Nr	Omschrijving
PFS-001	De oplossing voldoet aan pas toe of leg uit standaard Digitoegankelijk (EN 301 549 met WCAG 2.1).
PFS-002	De oplossing voldoet aan pas toe of leg uit standaard OpenAPI Specification.
PFS-003	De oplossing voldoet aan pas toe of leg uit standaard REST-API Design Rules.
PFS-004	De oplossing voldoet aan pas toe of leg uit standaard ICDD (NEN-EN-ISO 21597).
PFS-005	De oplossing voldoet aan pas toe of leg uit standaard CMIS.
PFS-006	De oplossing voldoet aan pas toe of leg uit standaard ODF.
PFS-007	De oplossing voldoet aan pas toe of leg uit standaard PDF (NEN-ISO).

Nr	Omschrijving
PFS-008	De oplossing voldoet aan pas toe of leg uit standaard HTTPS en HSTS.
PFS-009	De oplossing voldoet aan pas toe of leg uit standaard TLS v1.3.
PFS-010	De oplossing voldoet aan pas toe of leg uit standaard IPv6.
PFS-011	De oplossing voldoet aan pas toe of leg uit standaard Ades Baseline Profiles.
PFS-012	De oplossing voldoet aan pas toe of leg uit standaard DKIM.
PFS-013	De oplossing voldoet aan pas toe of leg uit standaard DMARC.
PFS-014	De oplossing voldoet aan pas toe of leg uit standaard NEN-ISO/IEC 27001.
PFS-015	De oplossing voldoet aan pas toe of leg uit standaard NEN-ISO/IEC 27002.
PFS-016	De oplossing voldoet aan pas toe of leg uit standaard NL GOV Assurance profile for OAuth 2.0.
PFS-017	De oplossing voldoet aan pas toe of leg uit standaard RPKI.
PFS-018	De oplossing voldoet aan pas toe of leg uit standaard SAML.
PFS-019	De oplossing voldoet aan pas toe of leg uit standaard OpenID-Connect.
PFS-020	De oplossing voldoet aan pas toe of leg uit standaard SCIM.
PFS-021	De oplossing voldoet aan pas toe of leg uit standaard SPF.
PFS-022	De oplossing voldoet aan pas toe of leg uit standaard NCSC beveiligingseisen voor webapplicaties.

5 Informatiebeveiliging eisen

Toelichting

Over de invulling van de Informatiebeveiliging eisen maakt de opdrachtnemer afspraken. Deze kan bijvoorbeeld bestaan uit een derde partij Assurance met van toepassing zijnde scope, geldigheid en afgifte door een erkende instantie.

5.1 Actuele wetten en voorschriften

Eisen:

Nr	Omschrijving
AWV-001	De opdrachtnemer dient aantoonbaar te maken compliant te zijn aan de Baseline Informatiebeveiliging Overheid (BIO) of diens opvolgers.
AWV-002	De aangeboden oplossing voldoet aan de Algemene Verordening Gegevensbescherming (AVG). De opdrachtnemer toont dit aan door de GAP-analyse op basis van de Privacy Baseline CIP (2018) aan te leveren. ²
AWV-003	Zodra de NIS2 actief van toepassing is dient deze te worden nageleefd door opdrachtnemer.

5.2 CIS³ & ABDO Controls⁴

Eisen:

Nr	Omschrijving
CAC-001	Opdrachtnemer is verantwoordelijk om, waar noodzakelijk, onderstaande CIS en ABDO controls samen met de hostingpartij in te richten en hierover te rapporteren. Het is aan opdrachtnemer om dit in te regelen en volledig te zijn.
CAC-002	CIS Control 3.10: <i>"Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH)."</i>

² https://www.cip-overheid.nl/media/y1kbux5w/gap-analyse-privacy-versie-13_model_cip.xlsx

³ CIS Controls Version 8

⁴ ABDO Algemene Beveiligingseisen voor Defensieopdrachten 2019

Nr	Omschrijving
CAC-003	CIS Control 3.11: <i>"Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include applicationlayer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data."</i>
CAC-004	CIS Control 7.1: <i>"Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."</i>
CAC-005	CIS Control 7.2: <i>"Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews."</i>
CAC-006	CIS Control 7.3: <i>"Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis."</i>
CAC-007	CIS Control 7.4: <i>"Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis."</i>
CAC-008	CIS Control 7.7: <i>"Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process."</i>
CAC-009	CIS Control 8.1: <i>"Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."</i>
CAC-010	CIS Control 8.2: <i>"Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets."</i>
CAC-011	CIS Control 8.4: <i>"Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported."</i>

Nr	Omschrijving
CAC-012	CIS Control 8.5: <i>"Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation."</i>
CAC-013	CIS Control 8.6: <i>"Collect DNS query audit logs on enterprise assets, where appropriate and supported."</i>
CAC-014	CIS Control 8.7: <i>"Collect URL request audit logs on enterprise assets, where appropriate and supported."</i>
CAC-015	CIS Control 8.8: <i>"Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals."</i>
CAC-016	CIS Control 8.9: <i>"Centralize, to the extent possible, audit log collection and retention across enterprise assets."</i>
CAC-017	CIS Control 8.10: <i>"Retain audit logs across enterprise assets for a minimum of 90 days."</i>
CAC-018	CIS Control 8.11: <i>"Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat."</i>
CAC-019	CIS Control 8.12: <i>"Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events."</i>
CAC-020	CIS Control 13.4: <i>"Perform traffic filtering between network segments, where appropriate."</i>
CAC-021	CIS Control 13.6: <i>"Collect network traffic flow logs and/or network traffic to review and alert upon from network devices."</i>
CAC-022	CIS Control 13.10: <i>"Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway."</i>
CAC-023	CIS Control 13.11: <i>"Tune security event alerting thresholds."</i>

Nr	Omschrijving
CAC-024	CIS Control 16.1: <i>"Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."</i>
CAC-025	CIS Control 16.2: <i>"Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard."</i> <i>Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders."</i>
CAC-026	CIS Control 16.3: <i>"Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise."</i>
CAC-027	CIS Control 16.4: <i>"Establish and manage an updated inventory of third-party components used in development, often referred to as a "bill of materials," as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported."</i>
CAC-028	CIS Control 16.5: <i>"Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use."</i>

Nr	Omschrijving
CAC-029	CIS Control 16.6: <i>"Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually."</i>
CAC-030	CIS Control 16.7: <i>"Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening."</i>
CAC-031	CIS Control 16.8: <i>"Maintain separate environments for production and non-production systems."</i>
CAC-032	CIS Control 16.9: <i>"Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers."</i>
CAC-033	CIS Control 16.10: <i>"Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of "never trust user input." Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts."</i>

Nr	Omschrijving
CAC-034	CIS Control 16.11: <i>"Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs."</i>
CAC-035	CIS Control 16.12: <i>"Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed."</i>
CAC-036	CIS Control 16.13: <i>"Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user."</i>
CAC-037	CIS Control 16.14: <i>"Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses."</i>
CAC-038	CIS Control 17.1: <i>"Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard."</i>
CAC-039	CIS Control 17.2: <i>"Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date."</i>

Nr	Omschrijving
CAC-040	CIS Control 17.3: <i>"Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard."</i>
CAC-041	CIS Control 18.1: <i>"Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements."</i>
CAC-042	CIS Control 18.2: <i>"Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box."</i>
CAC-043	CIS Control 18.3: <i>"Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization."</i>
CAC-044	CIS Control 18.4: <i>"Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing."</i>
CAC-045	CIS Control 18.5: <i>"Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box."</i>
CAC-046	ABDO Control 2.3.5: <i>"Na het beëindigen van de overeenkomst zijn alle digitale TBB teruggegeven aan opdrachtgever"</i>
CAC-047	ABDO Control 4.5.27: <i>"Toegangsrechten zijn periodiek, minimaal jaarlijks, geëvalueerd. Het interval is beschreven in het Beveiligingsplan."</i>
CAC-048	ABDO Control 4.8.3: <i>"Systeemcomponenten - zoals Firewall, router, switches, servers - zijn in de basis ingericht volgens een standaard configuratie. Deze configuratie is vastgelegd en regelmatig gecheckt op actualiteit."</i>

Nr	Omschrijving
CAC-049	ABDO Control 4.8.12: <i>"Ontwikkelaars hebben gescheiden gebruiksprofielen voor Ontwikkeling, Test, Acceptatie en Productiesystemen om het risico van fouten te verminderen. Het moet duidelijk zichtbaar zijn in welk systeem gewerkt wordt."</i>
CAC-050	ABDO Control 4.8.13: <i>"Indien er een experimenteer- of laboratorium omgeving is, is deze fysiek gescheiden van de andere omgevingen."</i>
CAC-051	ABDO Control 4.8.15: <i>"Gegevens uit de productieomgeving zijn alleen in de Acceptatieomgeving in gebruik wanneer deze op dezelfde wijze beveiligd zijn als in de productieomgeving. Deze gegevens zijn niet in een Ontwikkel- of Testomgeving gebruikt."</i>

5.3 MDR, Logging en monitoring

Eisen:

Nr	Omschrijving
MLM-001	Er dient een MDR oplossing te komen die CIS Controls 13.1, 13.2, 13.3, 13.7, 13.8 omvat. In afstemming tussen opdrachtnemer en opdrachtgever dient een MDR oplossing gekozen te worden passend bij de wens van opdrachtgever. De MDR oplossing zal apart aanbesteed worden en dient aansluiting te kunnen vinden op de oplossing van de opdrachtnemer.
MLM-002	De auditlogbestanden worden gedurende een voorgeschreven periode bewaard ten behoeve van toekomstig onderzoek.
MLM-003	De opdrachtnemer rapporteert maandelijks over security gebeurtenissen aan opdrachtgever (trendanalyse in algemene zin en eigen applicatie).
MLM-004	De opdrachtnemer dient opslag van en toegang tot logbestanden te reguleren en beveiligen middels de gangbare principes van privacy by design.

5.4 Toekomstige ontwikkelingen

Eisen:

Nr	Omschrijving
TO-001	De opdrachtnemer adviseert de opdrachtgever tijdig over marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over strategische ontwikkeling en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.

Nr	Omschrijving
TO-002	Opdrachtnemer moet op kunnen schalen naar quantum-proof/ready encryptie algoritme standaarden indien deze beschikbaar zijn. Tot die tijd moet opgeschaald kunnen worden naar een hybride constructie tussen klassieke cryptografie (elliptische curve of RSA) en post-quantum cryptografie.

5.5 Autorisatie

Eisen:

Nr	Omschrijving
AT-001	Sessies zijn authentiek en worden ongeldig gemaakt c.q. beëindigd conform ingestelde time-out of perioden van inactiviteit.
AT-002	De oplossing biedt automatische mechanismen om niet-vertrouwde bestandsgegevens, al dan niet uit niet-vertrouwde omgevingen, veilig te importeren en veilig op te slaan.
AT-003	De oplossing is zo ingericht dat de informatieobjecten en de metadata van die informatieobjecten zijn beschermd tegen toegang, wijziging of vernietiging door onbevoegden.
AT-004	De oplossing hanteert het Principle of least privilege. Dit betekent dat elke rol alleen toegang heeft tot de systeemmiddelen die nodig zijn voor het uitvoeren van de rol.

5.6 Diensten van derden

Eisen:

Nr	Omschrijving
DVD-001	Voor alle softwarecomponenten en diensten (van derden) binnen de oplossing draagt opdrachtnemer er zorg voor dat deze minimaal hetzelfde beveiligingsniveau kennen zoals gesteld aan de software en diensten die door opdrachtnemer worden geleverd.

5.7 Omgevingen

Eisen:

Nr	Omschrijving
OG-001	Alle omgevingen van de opdrachtgever zijn logisch te scheiden van andere omgevingen.
OG-002	Opdrachtnemer garandeert dat (meta)data van opdrachtgever niet buiten de Europese Economische Ruimte (EER) opgeslagen, beheerd, ingezien, verwerkt of bewerkt wordt.
OG-003	De gegevens van opdrachtgever dienen enkel toegankelijk te zijn voor de door opdrachtgever geautoriseerde personen.

5.8 Privacy supplementen

Eisen:

Nr	Omschrijving
PS-001	De (fysieke) beveiliging van omgevingen waar persoonsgegevens (en overige data) worden verwerkt, zijn op passende wijze ingericht zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen.
PS-002	De toegang tot de (fysieke) omgevingen wordt geregistreerd en er wordt gelogd op beheerderstoegang en -activiteiten. Deze eis geldt ook voor data in transit en data in rest.
PS-003	Opdrachtnemer garandeert dat een ieder die toegang krijgt, zowel fysiek als digitaal, of toegang heeft tot de data en omgeving van de opdrachtgever spiegelt aan het vertrouwensniveau van opdrachtgever.
PS-004	Alle subverwerkers van de opdrachtnemer houden zich aan dezelfde standaarden en eisen als de opdrachtnemer.
PS-005	De opdrachtnemer laat jaarlijks een privacy-audit uitvoeren door een gecertificeerde externe partij. Eventuele bevindingen die niet vooraf zijn afgestemd worden door opdrachtnemer op eigen kosten weggewerkt.
PS-006	Opdrachtgever heeft het right-to-audit op opdrachtnemer.

5.9 Controle op naleving en melding incidenten

Eisen:

Nr	Omschrijving
CN-001	Opdrachtnemer controleert informatiesystemen tenminste jaarlijks op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid, bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten en rapporteert daarover aan opdrachtgever. Het mitigeren of accepteren van risico's gebeurt op basis van een risicoafweging - waar nodig in afstemming met opdrachtgever - en opdrachtnemer rapporteert daarover aan opdrachtgever.

6 Integratie-eisen

6.1 Netwerkttoegang

Toelichting

Het Content Services Platform moet worden benaderd vanuit verschillende werkplekconcepten (SSC-ICT, RWS CIV en SSC-Campus). Elk van die concepten voorziet in de aansluiting op specifieke overheidsnetwerken. Door de oplossing eenmalig te ontsluiten op zo'n overheidsnetwerk (bijvoorbeeld het Rijksweb op de Haagse Ring, of het WAN-i netwerk) hebben alle werkplekconcepten zonder decentrale aanpassingen toegang.

Eisen:

Nr	Omschrijving
IGE-001	De oplossing is in staat door eenmalig te ontsluiten op een overheidsnetwerk toegang te geven aan alle genoemde werkplekconcepten zonder decentrale aanpassingen.
IGE-002	De oplossing voldoet aan IDWOR uitwerking-kader-8-werkplekonafhankelijkheid-van-klantapplicaties-v1.0.pdf (overheid-i.nl) .
IGE-003	De oplossing sluit aan op het Rijksoverheids Netwerk zodat alle gebruikersinterfaces via dit netwerk zijn te benaderen.
IGE-004	De oplossing is benaderbaar voor niet standaard werkplekken in Azure of AWS.

6.2 Koppelpunt informatie-uitwisseling

Toelichting

Interactie tussen diensten verloopt via een centraal koppelpunt. Dit koppelpunt bevat twee soorten diensten: 1) diensten voor uitwisselen van berichten via queues en 2) een portaal naar de verschillende webservices van diensten.

Eisen:

Nr	Omschrijving
KIU-001	De oplossing ontsluit alle opgeleverde diensten afzonderlijk via een koppelpunt informatie-uitwisseling.
KIU-002	Alle asynchrone uitwisseling tussen diensten (services) verloopt via berichtenwachtrijen.
KIU-003	Alle synchrone uitwisseling tussen diensten (services) verloopt via restful WebAPI's.

7 Non-functionele eisen

7.1 Prestatie-efficiëntie

Toelichting

Zijn de prestaties in verhouding tot de hoeveelheid gebruikte middelen.

Eisen:

Nr	Omschrijving
PSE-001	De oplossing ondersteunt minimaal 5.000 gelijktijdige gebruikers zonder performance verlies en opdrachtnemer toont dit aan door middel van stresstestrapporten en monitoring.
PSE-002	De oplossing reageert in meer dan 95% van standaard bevestigingen (bijvoorbeeld openen informatieobject, eenvoudige zoekvragen en opslaan informatieobject) snel. • Snel: 0s < response-tijd < 2s • Goed: 2s < response-tijd < 5s • Matig: 5s < response-tijd < 10s • Traag: response-tijd > 10s
PSE-003	De oplossing heeft geen technische limiet ten aanzien van het aantal informatieobjecten en aantal versies.
PSE-004	De oplossing heeft geen beperking tot ten minste 250 GB voor het opslaan van verschillende types en grootten van bestanden (zoals officebestanden, audiovisuele bestanden, e-mails incl. bijlagen etc.).

7.2 Bruikbaarheid

Toelichting

De mate waarin een product of systeem gebruikt kan worden door gespecificeerde gebruikers om effectief, efficiënt en naar tevredenheid gespecificeerde doelen te bereiken in een gespecificeerde gebruikscontext.

Eisen:

Nr	Omschrijving
BKB-001	De gebruikersinterface geeft een duidelijke Nederlandse terugkoppeling/interactie richting de gebruiker nadat een actie uitgevoerd is in geval het proces correct verloopt (bijvoorbeeld uitvoeren zoekactie) en in negatieve zin als een fout optreedt (bijvoorbeeld invoercontrole).
BKB-002	De oplossing voldoet aan de IenW huisstijl van het Rijk, tenzij vanuit technisch oogpunt de huisstijl niet toereikend is. Bij afwijking wordt in overleg getreden met opdrachtgever. Zie voor aanvullende informatie over de huisstijl: www.rijkshuisstijl.nl .
BKB-003	De oplossing biedt de mogelijkheid om persoonlijke voorkeuren in te stellen door een gebruiker (bijvoorbeeld zoekvragen, favorieten en gepersonaliseerde weergaven van informatieobjecten).

Nr	Omschrijving
BKB-004	De gebruikersinterface, inclusief helpfunctie en documentatie, is volledig Nederlands.
BKB-005	De oplossing voldoet aan de toegankelijkheidseisen in de WCAG 2.1 level A + AA (of WCAG 2.2 A + AA en opvolgers indien deze in werking is en dus verplicht voor overheden).
BKB-006	De oplossing voldoet bij configuratie, inrichting en doorontwikkeling aan de digitale toegankelijkheidseisen op basis van het 'Tijdelijk besluit digitale toegankelijkheid overheid' ⁵ (in 2023 geborgd in de wet digitale overheid, Wdo) volgens de richtlijn WCAG 2.1 A + AA (of WCAG 2.2 A + AA indien deze al in werking is en dus verplicht voor overheden). Inrichting gebeurt in overleg met de opdrachtgever.
BKB-007	De digitale toegankelijkheid van de oplossing wordt door opdrachtnemer jaarlijks (en tussentijds bij grote wijzigingen) getoetst door een gecertificeerde externe partij. Eventuele bevindingen (afwijking van de op dat moment geldende (voor overheden verplichte) versie van de WCAG) die niet vooraf zijn afgestemd, worden door opdrachtnemer op eigen kosten weggewerkt. De opdrachtgever kan faciliteren in het leveren van expertise tijdens de realisatie van de oplossing en voor de toets. Opdrachtgever laat de digitale toegankelijkheid van de oplossing zelf ook toetsen. Ook hiervoor geldt dat eventuele bevindingen (afwijking van de op dat moment geldende (voor overheden verplichte) versie van de WCAG die niet vooraf zijn afgestemd door opdrachtnemer op eigen kosten worden weggewerkt.

⁵ Zie: [wetten.nl - Regeling - Tijdelijk besluit digitale toegankelijkheid overheid - BWBR0040936](https://wetten.nl/Regeling-Tijdelijk-besluit-digitale-toegankelijkheid-overheid-BWBR0040936)

8 Beheer Content Services Platform

Binnen de SLA zijn overige relevante eisen en afspraken vastgelegd.

8.1 Diensten voor beheer van omgevingen

Doel van de dienst

Het doel van de dienst is:

- Alle functionaliteiten en techniek van de oplossing werken en blijven werken conform de specificaties van opdrachtnemer.
- Wijzigingen van de oplossing op een beheerste en gecontroleerde manier releasematig doorgevoerd door CFB. Vervolgens naar productie gebracht en in beheer genomen.
- Gebruikers worden bij de uitvoering van de bedrijfsprocessen veilig en ongehinderd ondersteund door de oplossing en beschikken daarbij over betrouwbare en actuele gegevens.

Omschrijving van de dienst

Deze dienst betreft het beheer van de productie-, educatie- en acceptatieomgeving van de oplossing.

Eisen:

Nr	Omschrijving
DBO-001	De opdrachtnemer biedt actieve monitoring op (dreigende) verstoringen en foutmeldingen ten aanzien van continuering van de geboden dienstverlening en indien noodzakelijk herstel met signalering.
DBO-002	De opdrachtnemer biedt monitoring van de performance van de oplossing met signalering bij verstoringen als continu proces.
DBO-003	De opdrachtnemer voert het beschikbaar stellen uit en ondersteunt het in beheer nemen van nieuwe releases met daarbinnen: - Onderhouds- en releasekalender - Actuele documentatie en releasenotes - Testscripts en resultaten van unit- en systeemtesten - Geaccordeerde acceptatietest
DBO-004	De opdrachtnemer past Continuous Integration toe bij het beschikbaar stellen van nieuwe releases.
DBO-005	De opdrachtnemer past Continuous Delivery toe bij het beschikbaar stellen van nieuwe releases.
DBO-006	De oplossing biedt de mogelijkheid om een generieke basisversie (her te gebruiken functionaliteit zoals informatieobject acties) in te richten.
DBO-007	De oplossing biedt de mogelijkheid voor verschillende organisatieonderdelen de omgeving virtueel te scheiden.
DBO-008	De oplossing biedt de mogelijkheid om de generieke basisversie te verrijken met specifieke inrichting (bijvoorbeeld specifiek procesmodel) per organisatieonderdeel.

Nr	Omschrijving
DBO-009	De oplossing biedt de mogelijkheid om een virtuele OTAEP-omgeving ⁶ beschikbaar te stellen per organisatieonderdeel.
DBO-010	De oplossing biedt de mogelijkheid om een virtuele Educatie-omgeving of acceptatie omgeving beschikbaar te stellen per instantie.
DBO-011	De oplossing biedt de mogelijkheid de inhoud van keuzelijsten te beheren bij beschikbare metadatavelden.
DBO-012	De oplossing biedt de mogelijkheid om metadatering / invulvelden in te stellen ten aanzien van verplichting, presentatie, formaat en automatische invulling.
DBO-013	De oplossing biedt de mogelijkheid om processen te ondersteunen en hierbij onderdelen (velden, termijnen, sjablonen) te configureren.
DBO-014	De OTAE-omgevingen van de oplossing dienen geanonimiseerde data te bevatten.
DBO-015	De oplossing biedt de mogelijkheid om periodiek een geanonimiseerde kopie van een selectie van de data uit de Productie omgeving te maken gekoppeld aan releases ten behoeve van testdoeleinden.
DBO-016	De acceptatieomgeving van de oplossing is representatief voor de productieomgeving qua functionaliteit en performance.
DBO-017	De opdrachtnemer faciliteert het aanroepen van diensten van derden met een technisch test in een testomgeving door gebruik te maken van zelf te ontwikkelen stubs.

8.2 Diensten voor servicedesk

Doel van de dienst

Het doel van de dienst is dat er bij Opdrachtnemer een eenduidig benaderbaar contactpunt is voor meldingen.

Omschrijving van de dienst

De Servicedesk van opdrachtnemer:

- Is een single point of contact voor doorgezette meldingen.
- Is verantwoordelijk voor de afhandeling van doorgezette meldingen.

Onder een melding wordt verstaan een:

- Vraag om het leveren voor beheerwerkzaamheden (Service Requests)
- Verstoring
- Standaard wijziging
- Wijzigingsverzoek
- Vraag
- Impactanalyse

⁶ OTAEP = Ontwikkel, Test, Acceptatie, Educatie en Productie

Eisen:

Nr	Omschrijving
DVS-001	De servicedesk van opdrachtnemer is een single point of contact voor meldingen.
DVS-002	De servicedesk van opdrachtnemer is verantwoordelijk voor de afhandeling van meldingen en de proactieve communicatie hierbij conform SLA.
DVS-003	Over bovenstaande punten wordt transparant gerapporteerd in een Service Level Rapportage zoals opgenomen in SLA.

8.3 Diensten voor beheer autorisaties

Doel van de dienst

Het doel van de dienst is het beheren van autorisaties binnen de oplossing.

Omschrijving van de dienst

De dienst beheer autorisaties biedt de benodigde functionaliteit om de volgende acties op te pakken:

- Inrichten autorisatiegroepen
- Aanmaken gebruikers
- Toekennen rechten aan gebruikers
- Wijzigen rechten van gebruikers
- Verwijderen gebruikers
- Rapporteren over ingerichte autorisaties

Eisen:

Nr	Omschrijving
DBA-001	De oplossing biedt een module waarin gebruikers en autorisaties eenvoudig op één plek beheerd kunnen worden.
DBA-002	De oplossing biedt de mogelijkheid om test-gebruikers aan te maken ten behoeve van testen van rechten en uitvoeren van testen.
DBA-003	De oplossing biedt de mogelijkheid om gebruikersgegevens vanuit provisioning te verwerken gebruikmakend van een uniek kenmerk.
DBA-004	De oplossing biedt de mogelijkheid op rol gebaseerde autorisatie in te richten.
DBA-005	De oplossing biedt de mogelijkheid om groepen in te richten op basis van organisatie onderdeel, directie, samenstelling gebruikers en interne vertrouwelijkheden (bijvoorbeeld rubricering of merking toe te passen op niveau dossiers en/of informatieobjecten).
DBA-006	De oplossing biedt de mogelijkheid een overzicht in wijzigingen van de autorisaties te maken op basis van rollen en groepen.
DBA-007	De oplossing biedt de mogelijkheid om functionaliteit middels rechten wel/niet beschikbaar te stellen aan rollen en groepen.
DBA-008	De oplossing biedt de mogelijkheid om toegang te verlenen tot beheerrollen.

Nr	Omschrijving
DBA-009	De oplossing biedt de mogelijkheid om parafeerders en gemandateerden in te richten.
DBA-010	De oplossing biedt de mogelijkheid om gebruikers inactief te maken en dit per specifieke datum of per direct door te voeren.
DBA-011	De oplossing biedt de mogelijkheid om gebruikers te verwijderen en dit per specifieke datum of per direct door te voeren.
DBA-012	De oplossing waarborgt herleidbaarheid van acties naar gebruiker na verwijdering van een gebruiker.
DBA-013	De oplossing biedt de mogelijkheid om bij het intrekken van rechten de gegevens van gebruikers te behouden in de eigenschappen van het informatieobject.
DBA-014	De oplossing biedt de mogelijkheid een overzicht in autorisatiestructuur, algemene rechten en specifieke rechten te maken voor de gehele oplossing gerelateerd aan rollen en groepen.

9 Onderhoud Content Services Platform

Binnen de SLA zijn overige relevante eisen en afspraken vastgelegd.

9.1 Diensten voor preventief onderhoud

Doel van de dienst

Het doel van deze dienst is dat de oplossing blijft werken conform de geldende specificaties zoals uitgewerkt in dit PvE door preventieve maatregelen, zoals:

- Het voorkomen van mogelijke verstoringen.
- Het verhogen van de onderhoudbaarheid en verhogen van beheerbaarheid inclusief beveiligingsaspecten.
- Het behouden van leverancierssupport.

Omschrijving van de dienst

De Dienst Preventief onderhoud behelst het corrigeren van de oplossing zonder dat er een aanleiding is in de vorm van een verstoring of andere melding.

Eisen:

Nr	Omschrijving
DPO-001	Opdrachtnemer borgt het doorvoeren van (niet-functionele) patches en updates die ervoor zorgdragen dat de oplossing conform de specificaties werkt en blijft werken.
DPO-002	Opdrachtnemer borgt het doorvoeren van (niet-functionele) patches en updates die ervoor zorgdragen dat de oplossing betrouwbaar en veilig is en blijft.
DPO-003	Opdrachtnemer borgt dat de oplossing is ingericht met versies overeenkomstig de geldende instructies, waardoor de werking en leverancierssupport niet in gevaar komt.
DPO-004	Opdrachtnemer stemt vooraf met opdrachtgever af indien preventief onderhoud wordt uitgevoerd.

9.2 Diensten voor correctief onderhoud

Doel van de dienst

De dienst Correctief Onderhoud op de oplossing teneinde verstoringen te verhelpen en (repeterende) verstoringen te voorkomen.

Omschrijving van de dienst

Het doel van de dienst is het herstellen van de werking van de oplossing na het optreden van een verstoring.

Zie *Bijlage 1D Concept SLA* voor een nadere toelichting op de classificatie van verstoringen en bijbehorende Service Levels en normen.

Eisen:

Nr	Omschrijving
DCO-001	Opdrachtnemer analyseert de verstoring en koppelt de beoogde oplossing voor een verstoring of workaround terug aan opdrachtgever.
DCO-002	Opdrachtnemer borgt dat de analyse een Root Cause Analysis en maatregelen ter voorkoming van repeterende verstoringen bevat.
DCO-003	Opdrachtnemer communiceert proactief conform overeengekomen communicatielijnen over verstoringen.
DCO-004	Opdrachtnemer biedt de beoogde oplossing voor een verstoring ter acceptatie aan bij opdrachtgever en levert een testrapport van geaccordeerde testen aan in de T-omgeving.
DCO-005	Over bovenstaande punten wordt transparant gerapporteerd in een Service Level Rapportage zoals opgenomen in SLA.
DCO-006	Enkele dagen per kalenderjaar dienen verstoringen in de Productieomgeving ook buiten werktijden te worden opgelost. De planning van deze dagen wordt tijdig met opdrachtnemer afgestemd.

9.3 Diensten voor adaptief en perfectief onderhoud*Doel van de dienst*

Het doel van deze dienst is dat de oplossing conform de gewijzigde specificaties werkt. Het betreft specificaties gericht op configuratie van de oplossing en integratie met de oplossing.

Omschrijving van de dienst

Adaptief en perfectief onderhoud omvat het wijzigen van de oplossing op verzoek van opdrachtgever. Het betreft hier doorontwikkeling van de oplossing waarbij opdrachtgever vanuit de rol *Product owner* afstemt met opdrachtnemer.

Aan een verzoek kunnen onder andere de volgende redenen ten grondslag liggen:

- Standaard wijzigingen:
 - a. Kleine wijzigingen.
 - b. Frequent voorkomen.
- Niet-standaard wijzigingen:
 - a. Wijzigingen in de uitvoering van processen van Opdrachtgever.
 - b. Wijzigingen in wet- en regelgeving.
 - c. Wijzigingen in koppelingen met andere systemen (adaptief onderhoud).
 - d. Optimaliseren van bestaande functionaliteiten (perfectief onderhoud).

Aan deze dienst zijn de volgende eisen gesteld:

Nr	Omschrijving
DAPO-001	Opdrachtnemer werkt een impactanalyse uit, inclusief de kosten, doorlooptijd en een werkinstructie voor de uitvoering van de wijziging.
DAPO-002	Opdrachtnemer werkt voor complexe wijzigingen een functioneel ontwerp uit inclusief toets op architectuurkaders.

Nr	Omschrijving
DAPO-003	Opdrachtnemer realiseert een wijziging na akkoord van Opdrachtgever en borgt Continuous Integration en Continuous Delivery.
DAPO-004	Opdrachtnemer borgt een agile werkwijze bestaande uit sprint(s) met tijdsreservering
DAPO-005	Opdrachtnemer borgt actuele documentatie, opleidingsmateriaal en releasenotes bij het beschikbaar stellen voor Acceptatietest.
DAPO-006	Opdrachtnemer biedt een wijziging voor Acceptatietest aan in de A-omgeving voor akkoord opdrachtgever en levert een testrapport aan van geaccordeerde testen in de T-omgeving.
DAPO-007	Opdrachtnemer lost tijdens de Acceptatietest adequaat testbevindingen op en biedt deze uiterlijk binnen 2 werkdagen opnieuw aan voor hertest.
DAPO-008	Opdrachtnemer stelt de wijziging beschikbaar in de P-omgeving na akkoord Acceptatietest en conform overeengekomen releaseplanning met opdrachtgever.
DAPO-009	Opdrachtnemer monitort het wijzigingenproces actief op doorlooptijd en kwaliteitseisen en informeert opdrachtgever.
DAPO-010	Over bovenstaande punten wordt transparant gerapporteerd in een Service Level Rapportage zoals opgenomen in SLA.

10 Uitvoeringseisen

Hieronder staan de algemene eisen aan de uitvoering van de dienstvermelding vermeld.

Nr	Omschrijving
UIT-001	De opgegeven beschreven dienstverlening, aangeboden kwaliteit en tarieven gelden voor de gehele dienstverlening gedurende de looptijd van de overeenkomst.
UIT-002	Voor alle medewerkers van de opdrachtnemer en/of medewerkers die worden ingezet via de opdrachtnemer, die werkzaamheden uitvoeren op locatie van opdrachtgever en/of middels Remote Support worden ingezet dient een geldige VOG (Verklaring Omtrent Gedrag), VGB (indien van toepassing, de verklaring Van Geen Bezwaar) en geheimhoudingsverklaring van tevoren te worden overlegd aan opdrachtgever. In geval van inzet medewerkers in het buitenland betreft het een gelijkwaardige verklaring.
UIT-003	Opdrachtnemer is akkoord met het feit dat de beheerwerkzaamheden in de loop van de tijd kunnen afnemen door standaardisatie en procesoptimalisaties van de door opdrachtgever uitgevraagde dienstverlening.
UIT-004	Opdrachtnemer is akkoord met de effecten van de gevraagde schaalbaarheid (aantal gebruikers, data volumes en benodigde performance kunnen door de tijd heen fluctueren); Opdrachtnemer heeft afdoende mogelijkheden beschikbaar om capaciteit (mensen en middelen) tijdig op en af te schalen, waar en wanneer nodig.
UIT-005	Communicatie tussen opdrachtnemer en opdrachtgever dient plaats te vinden in het Nederlands, zowel in woord als in geschrift.
UIT-006	Opdrachtnemer gaat er mee akkoord dat aansturing van de dienstverlening door een door opdrachtgever nog te selecteren dienstverlener namens opdrachtgever uitgevoerd kan worden.
UIT-007	Opdrachtnemer dient in leesbaar en bewerkbaar formaat informatie aan te leveren ten behoeve van interne auditprocedures en haar administratieve systeem van opdrachtgever. Dit betreft informatie over de geleverde dienstverlening waaronder configuratie, hard- en software, netwerk, certificaten, interfaces en contactpersonen. Deze aangeleverde informatie dient door opdrachtgever geautomatiseerd in te lezen te zijn in haar rapportagesysteem.
UIT-008	Opdrachtnemer dient gezamenlijk met de regieorganisatie tijdens de Implementatie templates op te stellen voor gebruik tijdens ontwikkeling conform de door opdrachtnemer voorgestelde projectmethodiek (Agile werkwijze).
UIT-009	Alle documentatie, inclusief draaiboeken en werkinstructies ten behoeve van beheer-, test- en onderhoudsactiviteiten, die betrekking heeft op de dienstverlening door opdrachtnemer aan opdrachtgever, dient gedurende de contractperiode door opdrachtnemer up-to-date gehouden te worden.

Nr	Omschrijving																																	
UIT-010	Opdrachtnemer is verantwoordelijk voor het beheer van de SLA die is afgestemd met opdrachtgever.																																	
UIT-011	Opdrachtnemer dient bij (dreigende) onbeschikbaarheid of performance issues in de keten actief mee te werken aan het oplossen van het mogelijke probleem binnen de gestelde termijn. Dit is onderdeel van de standaard dienstverlening.																																	
UIT-012	Opdrachtnemer is verantwoordelijk voor het beheer van de DFA welke na gunning gezamenlijk met opdrachtgever wordt opgesteld.																																	
UIT-013	Opdrachtnemer is verantwoordelijk voor het beheer van de PDC die is afgestemd met opdrachtgever.																																	
UIT-014	Opdrachtnemer conformeert zich aan de beleidsuitgangspunten van Opdrachtgever zoals vastgelegd in de <i>Bijlage 2</i> PSA.																																	
UIT-015	Opdrachtnemer is akkoord met de voorwaarde dat het gebruik van nieuwe technologie en/of maatwerk pas wordt toegepast na afstemming met en goedkeuring door opdrachtgever.																																	
UIT-016	Opdrachtnemer garandeert dat standaard-oplossingen worden uitgeleverd en onderhouden.																																	
UIT-019	Opdrachtnemer stemt ermee in dat de Migratie (de technische overgang van het CSP), als onderdeel van de Implementatie, maximaal drie opeenvolgende werkdagen omvat en niet mag plaatsvinden in de volgende periodes (exacte data worden na gunning vastgesteld): <table><tr><td>1 Vragen jaarverslag</td><td>FEZ</td><td>Eind mei</td></tr><tr><td>1 Vragen Slotwet</td><td>FEZ</td><td>Eind mei</td></tr><tr><td>2 1e Suppletoire wet</td><td>FEZ</td><td>Medio Juni</td></tr><tr><td>3 Schriftelijke begrotingsvragen</td><td>FEZ</td><td>Twee weken in oktober</td></tr><tr><td>4 Mondelinge begrotingsvragen</td><td>DBO</td><td>1 dag in November</td></tr><tr><td>5 2e Suppletoire wet</td><td>FEZ</td><td>Eerste helft december</td></tr><tr><td>6 Algemene pol. beschouwingen Tweede Kamer</td><td>DBO</td><td>Derde dinsdag september</td></tr><tr><td>7 Algemene pol. beschouwingen Eerste Kamer</td><td>DBO</td><td>Medio oktober</td></tr><tr><td>8 Verantwoordingsdebat</td><td>DBO</td><td>Derde woensdag in mei</td></tr><tr><td>Recessen</td><td>DBO</td><td>Gedurende twee weken voorafgaand aan een reces.</td></tr><tr><td>Spoeddebatten n.a.v. incidenten</td><td>DBO</td><td>Incidenteel</td></tr></table>	1 Vragen jaarverslag	FEZ	Eind mei	1 Vragen Slotwet	FEZ	Eind mei	2 1e Suppletoire wet	FEZ	Medio Juni	3 Schriftelijke begrotingsvragen	FEZ	Twee weken in oktober	4 Mondelinge begrotingsvragen	DBO	1 dag in November	5 2e Suppletoire wet	FEZ	Eerste helft december	6 Algemene pol. beschouwingen Tweede Kamer	DBO	Derde dinsdag september	7 Algemene pol. beschouwingen Eerste Kamer	DBO	Medio oktober	8 Verantwoordingsdebat	DBO	Derde woensdag in mei	Recessen	DBO	Gedurende twee weken voorafgaand aan een reces.	Spoeddebatten n.a.v. incidenten	DBO	Incidenteel
1 Vragen jaarverslag	FEZ	Eind mei																																
1 Vragen Slotwet	FEZ	Eind mei																																
2 1e Suppletoire wet	FEZ	Medio Juni																																
3 Schriftelijke begrotingsvragen	FEZ	Twee weken in oktober																																
4 Mondelinge begrotingsvragen	DBO	1 dag in November																																
5 2e Suppletoire wet	FEZ	Eerste helft december																																
6 Algemene pol. beschouwingen Tweede Kamer	DBO	Derde dinsdag september																																
7 Algemene pol. beschouwingen Eerste Kamer	DBO	Medio oktober																																
8 Verantwoordingsdebat	DBO	Derde woensdag in mei																																
Recessen	DBO	Gedurende twee weken voorafgaand aan een reces.																																
Spoeddebatten n.a.v. incidenten	DBO	Incidenteel																																
UIT-017	Opdrachtnemer is eindverantwoordelijk voor integrale succesvolle uitvoering van de implementatie																																	

Nr	Omschrijving
UIT-018	Opdrachtnemer dient de beschikbaarheid, integriteit en vertrouwelijkheid van data te allen tijde te garanderen.
UIT-020	Opdrachtnemer garandeert dat bij de start van de implementatie en migratie een projectorganisatie operationeel is die de implementatie en migratie succesvol doet verlopen en de, in afstemming met opdrachtgever, regie voert over (de ondersteuning tijdens) de implementatie en migratiefase.
UIT-021	Wanneer de migratie op onderdelen niet succesvol is dient Opdrachtnemer de uitvoering en coördinatie van een eventuele fallback op basis van het migratieplan op zich te nemen. Opdrachtnemer is verantwoordelijk voor het uitvoeren van het vooraf geaccepteerde Fallback-plan en stuurt hierbij de latende leverancier en opdrachtgever aan.
UIT-022	Opdrachtnemer dient gedurende de duur van de overeenkomst zoveel mogelijk vaste contactpersonen in te zetten met een vaste vervanging op operationeel niveau.
UIT-023	Opdrachtnemer verzorgt de vastlegging van reguliere overleggen (operationeel, tactisch en strategisch) en deelt deze met de betrokken contactpersonen.
UIT-024	Opdrachtnemer dient maandelijks een operationeel overleg voor te bereiden, te plannen en bij te wonen waarin de rapportages voor de geleverde dienstverlening van de afgelopen maand worden besproken en beoordeeld.
UIT-025	Opdrachtnemer dient maandelijks een tactisch overleg voor te bereiden, te plannen en bij te wonen waarin het rapport voor de dienstverlening van de afgelopen maand op tactisch niveau wordt besproken en beoordeeld.
UIT-026	Opdrachtnemer dient minimaal een keer per kwartaal een strategisch overleg voor te bereiden, te plannen en bij te wonen.