Nummer	Categorie	Beschrijving functionele eisen
FE-01	Administration and Reporting	De Oplossing biedt de mogelijkheid voor beheerders om toegestane bestandsformaten te bepalen.
FE-02	Administration and Reporting	De Oplossing zorgt voor de beschikbaarheid van de logs voor de beheerder.
FE-03	Content Creation and Collaboration	De Oplossing ondersteunt een automatische toekenning van metadata van huidig naar nieuw CSP, waarbij de ontbrekende metadata automatisch worden gevuld op basis van default waarden.
FE-04	Content Creation and Collaboration	De Oplossing moet tijdens het importeren en exporteren van grote hoeveelheden externe en bestaande legacy-inhoud de structurele integriteit van de inhoud behouden, samen met alle bestaande metadata van alle informatieobjecten, inclusief beveiliging, machtigingen, relaties en afhankelijkheden.
FE-05	Content Creation and Collaboration	De Oplossing ondersteunt dat een gebruiker (beheerder) in kennis wordt gesteld (notificatie) bij een mislukte import en export.
FE-06	Content Creation and Collaboration	De Oplossing biedt minimaal twee keuzes voor de waarschuwingsmethode bij mislukte in-, en export, zoals e-mail, SMS of pushnotificatie
FE-07	Content Creation and Collaboration	De Oplossing ondersteunt dat een gebruiker met de juiste/voldoende rechten annotaties aan het betreffende informatieobject kan toevoegen en wijzigen.
FE-08	Document access control	De Oplossing moet een classificatiehiërarchie kunnen definiëren voor het toepassen van beveiliging en machtigingen op inhoud.
FE-09	Document access control	De Oplossing ondersteunt dat rechten, beperkingen en gedragingen kunnen worden geërfd van ouderclassificaties naar kindclassificaties in de hiërarchie.
FE-10	Document access control	De interface van de Oplossing moet beveiligd zijn, zodat gebruikers geen inhoud kunnen zien waartoe zij geen rechten hebben.
FE-11	Document access control	De Oplossing ondersteunt dat de toegang tot informatieobjecten en toegestane functionaliteit toegepast/ beperkt kan worden op basis van de object classificaties.
FE-12	Document access control	De Oplossing ondersteunt dat een Beveiligingshiërarchie gedefinieerd kan worden.
FE-13	Document access control	Binnen de Oplossing moeten toegangsrechten beheerd kunnen worden van gebruikers, gebruikersgroepen, en rollen op individueel informatie object niveau.
FE-14	Document access control	Binnen de Oplossing kunnen standaard beveiligingsclassificaties toegewezen worden aan informatie object types.
FE-15	Document access control	De Oplossing ondersteunt beveiligings- en toestemmingsbeperkingen op een bepaalde map/ dossier die gelden voor alle inhoud die op die locatie is opgeslagen.

FE-16	Document access control	De Oplossing ondersteunt dat een beheerder voorrangsregels kan instellen voor de verschillende beveiligingsinstellingen en -toewijzingen om mogelijke toegangsconflicten te voorkomen.
FE-17	Document access control	De Oplossing biedt de mogelijkheid aan beheerders of andere geautoriseerde gebruikers om de beveiligingsinstellingen te kunnen wijzigen van elk individueel content item, zoals een informatieobject.
FE-18	Document access control	De beheerder kan de rechten van een inhoudsgroep of aggregatie als eenheid aanpassen.
FE-19	Document access control	Het systeem moet middels een notificatie aangeven of een handeling in strijd is met de beveiligingsclassificaties.
FE-20	Library Services	De Oplossing levert unieke persistente identifiers die automatisch worden toegepast op alle informatieobjecten en structuurobjecten (aggregaties).
FE-21	Library Services	De Oplossing moet tenminste informatiesoorten en bestandsformaten ondersteunen met de volgende mime types: • Text/plain • Text/html • Text/xml • Application/pdf • Image/jpeg • Image/tiff En de informatiesoorten en bestandsformaten zoals gedefinieerd door het Nationaal archief (https://www.nationaalarchief.nl/sites/default/files/field-file/voorkeursformaten_nationaal_archief-v1.0.pdf)
FE-22	Library Services	De Oplossing moet voor de uitwisseling van gegevens met andere (internationale) instanties berichten in tenminste in XML en in JSON formaat te ondersteunen.

FE-23	Library Services	De Oplossing moet audio- en videobestanden ondersteunen zoals die zijn gedefinieerd bij het Nationaal archief (https://www.nationaalarchief.nl/sites/default/files/field-file/voorkeursformaten_nationaal_archief-v1.0.pdf) In aanvulling hierop moeten ook de volgende voorkeurs/acceptabele formaten ondersteund worden die voorzien zijn in de vervolgversie van het Nationaal Archief: Video: • codec XDCAM HD422 (voorkeur) • codec FFV1 (acceptabel) • codec H.264 (acceptabel) Audio: • codec LPCM (voorkeur) • codec FLAC (voorkeur) • codec MPEG-4 AAC/ALS (acceptabel)
FE-24	Library Services	De Oplossing ondersteunt dat een gebruiker inhoud, inclusief informatieobjecten, kan uitchecken voor bewerking. De uitcheckmogelijkheid voorkomt automatisch dat andere gebruikers de inhoud op enigerlei wijze wijzigen totdat deze weer is ingecheckt en door het systeem is vrijgegeven.
FE-25	Library Services	De Oplossing biedt de mogelijkheid dat de beheerder het volgende kan specificeren: • Welke inhoud onder versiebeheer valt, en • Hoeveel versies moeten worden bewaard.
FE-26	Library Services	De Oplossing ondersteunt dat terugdraaien naar vorige versies van de inhoud beschikbaar is.
FE-27	Library Services	De opslagstructuur van dossiers, informatieobjecten, content en andere objecten moet voldoen aan het metadatamodel van de SVB. De opslagstructuur is configureerbaar door de beheerder.
FE-28	Library Services	De Oplossing moet in staat zijn om meerdere gerelateerde informatieobjecten (samengesteld informatieobject) als een enkele eenheid te beheren.
FE-29	Library Services	De Oplossing ondersteunt dat een samengesteld informatieobject met een eigen unieke identifier (soms een documentenset genoemd) een willekeurig aantal informatieobjecten kan bevatten.
FE-30	Library Services	De Oplossing ondersteunt dat een samengesteld informatieobject metadata en gedrag over alle informatieobjecten binnen de documentenset deelt.
FE-31	Library Services	De Oplossing ondersteunt permanente referentiële integriteit voor alle relaties en afhankelijkheden tussen Informatieobjecten, ondanks wijzigingen in de inhoud en wijzigingen in de fysieke of logische opslaglocatie van de Informatieobjecten.

FE-32	Library Services	De Oplossing biedt de mogelijkheid dat een beheerder afzonderlijke stadia in de levenscyclus van een informatieobject of contentelement kan definiëren (bijvoorbeeld aangemaakt, herzien, gepubliceerd, vervangen en gearchiveerd).
FE-33	Library Services	De Oplossing ondersteunt dat een informatieobject kan worden verplaatst van een locatie (zoals een archief, bibliotheek of map) naar een andere locatie, waarbij de metadata van het informatieobject niet mag veranderen.
FE-34	Metadata and Classification	De Oplossing dient een Metadataschema te kunnen ondersteunen volgens de Nederlandse Overheidsstandaard MDTO. Hierin dienen tevens SVB specifieke aanpassingen doorgevoerd te kunnen worden.
FE-35	Metadata and Classification	De Oplossing moet metadata kunnen koppelen aan de individuele informatieobjecten die relaties gedurende de hele levenscyclus van de inhoud in stand houden
FE-36	Metadata and Classification	Metadata moeten worden vastgelegd als afzonderlijke waarden in afzonderlijke en onderscheiden velden voor elk beschreven inhoudsitem.
FE-37	Metadata and Classification	Het moet mogelijk zijn tenminste 100 zelf te definiëren metadatavelden te koppelen aan elk inhoudstype, naast eventuele vooraf gedefinieerde standaardmetadata.
FE-38	Metadata and Classification	Aggregaties die als een eenheid worden beheerd, zoals documentensets en recordreeksen, moeten metadata hebben die verband houden met de aggregatie als geheel (overerving).
FE-39	Metadata and Classification	De Oplossing kan metadata op verschillende aggregatieniveaus vaststellen.
FE-40	Metadata and Classification	De Oplossing ondersteunt dat een beheerder metadatavelden of elementen kan onderhouden.
FE-41	Metadata and Classification	De Oplossing ondersteunt dat een metadata-elementdefinitie minimaal bestaat uit een elementnaam, een beschrijving, een unieke identificatie en een waardeveld.
FE-42	Metadata and Classification	De Oplossing ondersteunt dat elk metadata element als een bepaald datatype kan worden opgegeven.
FE-43	Metadata and Classification	De Oplossing moet valideren dat de geleverde waarden overeenstemmen met het opgegeven datatype van een metadata-element.
FE-44	Metadata and Classification	De Oplossing biedt een centraal mechanisme voor het definieren en beheren van metadata.
FE-45	Metadata and Classification	De Oplossing ondersteunt dat de beheerder een metadata-element eenmaal kan definiëren en beschikbaar kan maken voor andere gebruikers en inhoud, met inachtneming van de toepasselijke rechten en bevoegdheidsbeperkingen.
FE-46	Metadata and Classification	De Oplossing biedt de mogelijkheid dat wanneer een wijziging in de definitie van een metadataelement moet worden doorgevoerd, de afzonderlijke metadata elementen niet apart nog moeten worden gewijzigd.

FE-47	Metadata and Classification	De Oplossing ondersteunt dat een bepaald metadata element in één context als verplicht en in een andere context als optioneel kan worden aangeduid.
FE-48	Metadata and Classification	De Oplossing kan op basis van vooraf gedefinieerde definities valideren dat metadata de juiste waarden heeft.
FE-49	Metadata and Classification	De Oplossing biedt de mogelijkheid dat het waardebereik van een metadataelement beperkt kan worden tot: • Een vooraf bepaalde lijst (voor tekstuele elementen) • Een waardebereik (voor numerieke elementen) • Een kalenderbereik (voor datumelementen)
FE-50	Metadata and Classification	De Oplossing biedt de mogelijkheid om een standaardwaarde (bv datum registratie) voor elk metadata veld in te voeren.
FE-51	Metadata and Classification	De Oplossing biedt de mogelijkheid dat metadatawaarden uit het bronsysteem na invoer worden vastgelegd en opgeslagen in het juiste metadataveld dat aan de inhoud is gekoppeld, zonder aangepaste ontwikkeling of een instrument van derden.
FE-52	Metadata and Classification	De Oplossing biedt de mogelijkheid bij integratie met een extern metadatabeheersysteem dat de eigen metadatabeheerfaciliteiten kunnen synchroniseren met de faciliteiten van het externe systeem.
FE-53	Records management	De Oplossing biedt de mogelijkheid tot verifieerbare (volgens te ondersteunen procedure) vernietiging van informatieobjecten op instructie en/of vanuit de informatiebeheerrichtlijnen.
FE-54	Records management	De Oplossing garandeert vernietiging van bestanden. Bij het volledig wissen van inhoud moet de Oplossing de volledige en onmiddellijke verwijdering van het inhoudsitem kunnen garanderen.
FE-55	Records management	De Oplossing biedt de mogelijkheid dat de logging moet aangeven wat is vernietigd, de datum van vernietiging, wie de vernietiging heeft goedgekeurd en de reden waarom de records zijn verwijderd, met verwijzing naar het relevante bewaarschema.
FE-56	Records management	Zodra inhoud tot record is verklaard, moet de Oplossing garanderen dat het inhoudsitem en de bijbehorende metadata niet kunnen worden gewijzigd, d.w.z. dat het record onveranderlijk moet zijn. Met uitzondering van metadata die als onderdeel van de record kan worden toegevoegd.
FE-57	Records management	Bevriezen en vasthouden van records: Een geautoriseerde gebruiker moet de voortgang van een record opheffen of opschorten. Deze opschorting moet de definitieve verwijdering van het record opheffen.
FE-58	Records management	De Oplossing biedt de mogelijkheid dat een geautoriseerde gebruiker in staat moet zijn de bevriezing van een record ongedaan te maken.
FE-59	Records management	De Oplossing biedt de mogelijkheid om de toegang van specifieke gebruikers tot inhoud te beperken op basis van de status van die inhoud in het bestandsschema of de classificatie (zie werking control access layers).
FE-60	Records management	De Oplossing moet records kunnen groeperen en beheren als recordsets en aggregaties, waarbij een aggregatie een willekeurig aantal records kan omvatten.

FE-61	Records management	De Oplossing biedt de mogelijkheid dat een enkel record tot meerdere recordsets of aggregaties kan behoren zonder dat er een kopie van het record moet worden gemaakt.
FE-62	Records management	De Oplossing kan eventuele conflicten automatisch oplossen indien een record, doordat het tot meerdere verzamelingen of aggregaties behoort, onder meerdere bewaarregels valt. De langste bewaartermijn wordt in acht genomen, en retentie en holds (vasthouden van record) voorkomen verwijderacties.
FE-63	Records management	De Oplossing biedt autorisaties aan meerdere gebruikers (beheerders) of systemen om te bepalen wanneer en hoe records van een bepaald type kunnen worden verwijderd.
FE-64	Records management	De Oplossing biedt de mogelijkheid dat meerdere gebruikers of meerdere systemen verwijderacties en gebeurtenissen kunnen opheffen of uitstellen.
FE-65	Search and Navigation	De Oplossing ondersteunt dat geautoriseerde gebruikers alle geïndexeerde inhoud kunnen doorzoeken en alle inhoud kunnen opvragen waartoe zij toegang hebben.
FE-66	Search and Navigation	De Oplossing ondersteunt een realtime verversingssnelheid van nieuwe inhoud.
FE-67	Search and Navigation	De Oplossing kan een herindexering toepassen indien de zoekindex corrupt raakt.
FE-68	Search and Navigation	De Oplossing biedt de mogelijkheid om full-tekst zoekopdrachten uit te voeren op metadata-elementen
FE-69	Search and Navigation	De Oplossing ondersteunt een zoekfunctie met AND, OR en NOT, en groepering door haakjes.
FE-70	Search and Navigation	De Oplossing ondersteunt zoeken op alle metadatavelden waarbij beperkingen kunnen worden ingegeven (voorwaardelijk kunnen zoeken).
FE-71	Search and Navigation	De Oplossing kan zoekresultaten filteren volgens de rechten van de gebruiker (zoeken met een beveiligd filter).
FE-72	Search and Navigation	De Oplossing kan de inhoud van de resultatenreeks van de zoekopdracht verder verfijnen (selectiefilter kunnen toepassen).

Nummer	Categorie	Beschrijving niet-functionele eisen
NF-00	Algemeen	De Oplossing is gebaseerd op standaard software een private cloud omgeving.
NF-01	Algemeen	De Oplossing en organisatie van Opdrachtnemer moet zijn beveiligd door het implementeren en onderhouden van een set van passende technische en organisatorische maatregelen welke de beschikbaarheid, integriteit en vertrouwelijkheid van de Oplossing en de daarop opgeslagen en/of verwerkte informatie borgt op ten minste industriestandaard wijze.
NF-02	Algemeen	De Opdrachtnemer vernietigt (voert af) media en/of ICT-componenten met vertrouwelijke SVB-informatie gerelateerd aan de levering van de gevraagde dienstverlening middels een formele procedure op een veilige manier.
NF-03	Algemeen	De Opdrachtnemer informeert de SVB, binnen het wettelijke kader, over verzoeken tot aanlevering van persoonsgegevens door buitenlandse inlichtingen- en opsporingsdiensten in het kader van de gevraagde dienstverlening.
NF-04	Algemeen	De Opdrachtnemer dient bij het ontwikkelen, implementeren en beheren van de Oplossing en de gevraagde dienstverlening rekening te houden met de principes "Security by Design (secure software development) en Security by Default", “Privacy by Design en Privacy by Default".
NF-05	Algemeen	Opdrachtnemer dient Informatiebeveiliging en bedrijfscontinuïteit gestandaardiseerd, gestructureerd en gebaseerd op een cyclus van continu verbeteren in de betreffende lagen van de organisatie en de te leveren Oplossing en dienstverlening te hebben ingericht (zie ook NF-13).
NF-06	Algemeen	De Opdrachtnemer moet een procedure hebben, uitvoeren en de resultaten rapporteren voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de gevraagde Oplossing en de dienstverlening. Dit dient periodiek, minimaal iedere 3 jaar, en daarnaast ook altijd opnieuw bij significante wijzigingen te gebeuren.
NF-07	Algemeen	Voor het uitvoeren van onderhoud en/of aanpassingen aan de Oplossing moet aantoonbaar een wijzigingsproces gehanteerd worden (“change management”) waarbij de nadruk ligt op het voorkomen van beveiligingsincidenten, storingen of onderbrekingen tijdens het doorvoeren van veranderingen.
NF-08	Algemeen	De Opdrachtnemer moet de SVB in staat stellen te kunnen voldoen aan (minimaal) de BBN-2 normen zoals beschreven in de huidige en opvolgende versies van de Baseline Informatiebeveiliging Overheid (BIO). Indien de BBN-classificatie in de BIO herijkt wordt, dan stelt de Opdrachtnemer de SVB in staat het BBN-niveau dat van de SVB vereist wordt te behalen (of te behouden)
NF-09	Rapportage	De Oplossing moet blijvend voldoen aan de geldende Nederlandse wet - en regelgeving.

NF-10	Authenticatie, autorisaties en vertrouwelijkheden	De Oplossing kan overweg met Role Based Access Control (RBAC): • Role claim: In de role claim worden alle rollen van de gebruiker (van alle applicaties) bij de applicatie aangeboden, EN • Role assignment: De rol van de gebruiker wordt aan een specifieke rechten claim toegewezen die de applicatie begrijpt.
NF-11	Authenticatie, autorisaties en vertrouwelijkheden	De Oplossing dient aan te sluiten op de standaard dienst (autorisatie): 'SVB eenmalig aanloggen' Nu gerealiseerd door Azure AD SSO/MFA (QS Solutions) alsmede op 1 van de verplichte standaarden van de overheid (PTOLU): SAML 2.0 of Oauth 2.0/OpenID Connect 1.0. Alternatief: WS-Federation v1.2
NF-12	Beheer	De Opdrachtnemer stelt in overleg met de SVB een Dossier Afspraken en Procedures (DAP) op.
NF-13	Beheer	De Opdrachtnemer stelt in overleg met de SVB een Business Continuity Plan (incl. Disaster Recovery plan and Backup and restore plan) op en zorgt teminste 1 keer per jaar voor een continuiteïtstest.
NF-14	Beheer	De Opdrachtnemer stelt in overleg met de SVB een Exit plan op waarin de continuiteit van de Oplossing en de werkzaamheden en verplichtingen bij het aflopen of beëindigen van de Overeenkomst vastgelegd worden.
NF-15	Beheer	De Opdrachtnemer stelt naast standaard documentatie van de Oplossing specifieke documentatie op met betrekking tot de specifieke implementatie van de Oplossing voor de SVB, conform de niet-functionele eisen.
NF-16	Beheer	De Opdrachtnemer voert Incident management en Problem management uit conform de niet-functionele eisen (zie ook NF-20 e.v. hierna).
NF-17	Beheer	De Opdrachtnemer voert Configuratiemanagement en Changemanagement uit conform de niet-functionele eisen (zie ook NF-20 e.v. hierna).
NF-18	Beschikbaarheid van de keten	De Opdrachtnemer moet de continuïteit van de Oplossing waarborgen, ook in geval van calamiteiten, rampen, hacking, systeeminbraak, verloren data, gegevensdiefstal en andere vormen van cybercriminaliteit.
NF-19	Beschikbaarheid van de keten (SLA)	De Oplossing moet 24/7 beschikbaar zijn met een beschikbaarheidspercentage van tenminste 99,5% voor de Productie omgeving, en tenminste 99,0% voor de Ontwikkel, Test, Acceptatie en Educatie omgevingen. Met beschikbaarheid wordt bedoeld: de totale tijdsduur waarin de eindgebruikers iedere maand daadwerkelijk (i.e. performant en overig in overstemming met de afgesproken eisen) gebruik hebben kunnen maken van de Oplossing. De beschikbaarheid wordt gemeten over iedere periode van één (1) kalendermaand. Gepland onderhoud mag op uitsluitend tussen 21:00u en 6:00u CET plaatsvinden behoudens voorafgaande en schriftelijke goedkeuring door de SVB.
NF-20	Beschikbaarheid van de keten (SLA)	Eindgebruikers (incl Beheerders) moeten de Oplossing vanaf een SVB-werkplek kunnen benaderen en de Oplossing kunnen gebruiken in overeenstemming met de afgesproken service levels.
NF-21	Beschikbaarheid van de keten (SLA)	Opdachtnemer zal een SLA beschikbaar stellen die onderdeel zal worden van de Overeenkomst die ten minste voldoet aan de eisen van dit programma van eisen (NF-20 e.v.).

NF-22	Beschikbaarheid van de keten (SLA)	Opdrachtnemer moet voorzien in passende technische en organisatorische maatregelen, waaronder monitoring, om incidenten in de productieomgeving van de Oplossing snel te kunnen detecteren, onderzoeken en op te lossen.
NF-23	Beschikbaarheid van de keten (SLA)	Opdrachtnemer zorgt voor back-up en restoremogelijkheden zodat er maximaal 8 uur dataverlies kan optreden en de oplossing niet langer dan 24uur onbeschikbaar is. Opdrachtnemer is verantwoordelijk voor controle van de integriteit van die back-ups, alsmede het waarborgen van de vertrouwelijkheid en beschikbaarheid daarvan. De eisen voor de Productie omgeving zijn: Recovery Point Objective = 8 uur Recovery Time Objective = 23 uur Work Recovery Time = 1 uur Maximum Tolerable Downtime = 24 uur De eisen voor de Ontwikkel, Test, Acceptatie en Educatie omgevingen zijn: Recovery Point Objective = 24 uur Recovery Time Objective = 22 uur Work Recovery Time = 2 uur Maximum Tolerable Downtime = 48 uur
NF-24	Beschikbaarheid van de keten (SLA)	De Opdrachtnemer heeft een single point of contact voor escalaties rondom communicatie met hun service desk en/of Incidenten, problems en andere verzoeken.
NF-25	Beschikbaarheid van de keten (SLA)	Opdrachtnemer moet voorzien in technische en organisatorische maatregelen, waaronder een incident management tool, voor het direct registeren, administreren en rapporteren van incidenten, problemen, wijzigingen, en vergelijkbare correspondentie. Opdrachtnemer zorgt ervoor dat de SVB te allen tijde toegang heeft tot die incidentmanagementtool en dat de SVB te allen tijde de status van incidenten, problemen, wijzigingen, en vergelijkbare correspondentie kan inzien.
NF-26	Beschikbaarheid van de keten (SLA)	Opdrachtnemer draagt zorgt voor de volledige infrastructuur van de Oplossing, waaronder de housing, hosting en het technisch beheer.
NF-27	Beschikbaarheid van de keten (SLA)	Opdrachtnemer dient in de SLA - in overleg met de SVB - de parameters te bepalen op basis waarvan de prioriteit van incidenten en problemen wordt vastgesteld (i.e. P1 tot en met P5). De prioritering dient te worden bepaald aan de hand van "scope impact x scope getroffen gebruikersgroep" (bij voorkeur uitgedrukt in een matrix). Voor incidenten en problemen m.b.t. informatiebeveiliging dient een aparte prioritering in de SLA te staan op basis van enkel "scope impact".

NF-28	Beschikbaarheid van de keten (SLA)	Opdrachtnemer hanteert tenminste de volgende respons- en oplostijden voor incidenten en problemen t.a.v. de productie-omgeving van de Oplossing: Prio 1: responsetijd < 10 min, en oplossing door Leverancier < 4 uur Prio 2: responsetijd < 1 uur, en oplossing door Leverancier < 8 uur Prio 3: responsetijd < 2 uur, en oplossing door Leverancier < 16 uur Prio 4: responsetijd <4 uur, en oplossing door Leverancier < 50 uur Prio 5: responsetijd < 8 uur, en oplossing door Leverancier < 120 uur Met responsetijd bedoeld de SVB een respons op basis van (1) het incident / probleem bekend is bij Leverancier; (2) het probleem binnen Leverancier belegd is; (3) leverancier aangegeven heeft dat informatie of medewerking vanuit SVB benodigd is. Ingeval van een P1 zal de leverancier per uur een update op de voortgang verstrekken aan SVB.
NF-29	Beschikbaarheid van de keten (SLA)	Eisen aan verbeterplan en Root Cause Analysis, deze moeten tenminste de onderstaande elementen bevatten (niet limitatief): • Beschrijving van het Incident of afwijking en het aantal (bij benadering) eindgebruikers dat hierdoor getroffen kan zijn • Beschrijving van de oorzaak van het Incident of afwijking • Beschrijving van de tijdelijke en of permanente oplossing • Beschrijving van de maatregelen die genomen zijn en zullen worden om zeker te stellen dat dit Incident of afwijking niet nogmaals plaatsvindt • Planning • Feiten en cijfers
NF-30	Beveiligingsincidenten	Opdrachtnemer heeft monitoring-, meld- en responsprocedures geïmplementeerd (en evalueert periodiek de effectiviteit daarvan) om informatiebeveiligingsincidenten (waaronder datalekken m.b.t. persoonsgegevens, inlogpogingen waarbij authenticatie mislukt) te detecteren, melden en de gevolgen daarvan te mitigeren.
NF-31	Beveiligingsincidenten	Opdrachtnemer (incl. onderaannemers) verleent medewerking bij het onderzoeken en oplossen van het informatiebeveiligingsincident en stelt, indien gevraagd, alle informatie met betrekking tot het incident (in het kader van de gevraagde dienstverlening) ter beschikking aan de SVB. De informatie dient minimaal 60 dagen na aanval nog beschikbaar te zijn. Deze informatie wordt ook beschikbaar gesteld bij eventueel onderzoek door een Derde partij.

NF-32	Beveiligingsincidenten	Log-bestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen (bijv. malicieuze activiteiten) registreren (ofwel loggings- en detectie-informatie), behoren te worden gemaakt, bewaard en regelmatig te worden geanalyseerd en beoordeeld door de Opdrachtnemer met betrekking tot alle onderdelen van de gevraagde Dienstverlening.
NF-33	Clouddiensten	De bij de Opdrachtnemer gebruikte encryptiesleutels voor het versleutelen van de data binnen de Oplossing moet op elk moment in het proces per direct overgedragen kunnen worden aan de SVB danwel ingetrokken of onbruikbaar gemaakt kunnen worden.
NF-34	Clouddiensten	a) Beveiligingscertificaten dienen bij de SVB ook zelf in beheer te kunnen worden genomen (zelf kunnen intrekken) b) De Oplossing dient ook om te gaan met door SVB gebruikte eigen sleutels voor de versleuteling van door de Oplossing opgeslagen inhoud.
NF-35	Clouddiensten	Opdrachtnemer zorgt ervoor dat alle door de SVB in de Oplossing ingevoerde metadata-objecten met metadata, relaties tussen metadata-objecten en Informatieobjecten exporteerbaar is in een gestructureerd en gangbaar bestandsformaat op zodanige wijze dat dit de SVB in staat stelt om de metadata-objecten met metadata, relaties tussen metadataobjecten en informatieobjecten zonder onredelijke inspanningen te porteren naar een andere (met Opdrachtnemer vergelijkbare) dienstverlener. In geval van aflopen of beëindiging van de Overeenkomst dient data van de SVB welke nog in het bezit is van De Opdrachtnemer na overdracht aan de SVB vervolgens op verzoek van de SVB conform daarvoor geldende internationale standaarden vernietigd te worden.
NF-36	Clouddiensten	Bij multi-tenancy worden alle gegevens die binnen de Oplossing worden opgeslagen of verwerkt ten behoeve van de SVB in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines.
NF-37	Clouddiensten	De Oplossing dient uitsluitend persoonsgegevens te verwerken, te transporteren en op te slaan binnen de Europese Economische Ruimte (EER).
NF-38	Controle & Audits	De SVB wordt geïnformeerd over de eventuele gebleken tekortkomingen m.b.t. beveiliging n.a.v. de door haar ingestelde beveiligingstest/-audits of onderzoek i.h.k.v. de gevraagde Oplossing en dienstverlening en deze dienen meegenomen te worden bij de doorontwikkeling van de Oplossing (als onderdeel van het Onderhoud) en zo nodig op de kortst mogelijke termijn te worden gepatcht.
NF-39	Documentatie	Opdrachtnemer stelt een functionele en technische handleiding beschikbaar van alle gebruikers- en beheerdersfunctionaliteit binnen de Oplossing, waaronder informatie over koppelingen, rapportages en gebruikersbeheer.
NF-40	Documentatie	Opdrachtnemer stelt een globale systeem schets van de gehele Oplossing ter beschikking.
NF-41	Documentatie	Bij elke Release wordt up to date documentatie in de Engelse of Nederlandse taal van tevoren beschikbaar gesteld over de wijzigingen van de Release en is de documentatie van het gebruik van de tool geupdate voor alle handleidingen.

NF-42	Eisen aan personeel	Alle medewerkers van Opdrachtnemer die participeren in de levering van de gevraagde dienstverlening moeten aantoonbaar bekend zijn met de overeengekomen verplichtingen op het gebied van informatiebeveiliging en bescherming van persoonsgegevens. In dit kader is er: • Een geheimhoudingsovereenkomst (NDA) ondertekend door Opdrachtnemer en wordt op basis daarvan gehandeld • Hebben alle medewerkers die participeren in de levering van de gevraagde dienstverlening en in aanraking komen met vertrouwelijke informatie van de SVB een specifiek voor de functie verstrekte Verklaring Omtrent Gedrag (VOG), of een gelijkwaardig document (in geval van een andere lidstaat), welke geldig is tijdens de duur van de Overeenkomst c.q. uitvoering van de werkzaamheden.
NF-43	Formaat exportdata voor BI	De Oplossing exporteert metadata-objecten met metadata en informatieobjecten voor aanlevering aan een analyse & rapportage omgeving, minimaal naar een bestand in CSV-formaat of een ander standaard formaat dat gangbaar is in de praktijk.
NF-44	Hosting	Opdrachtnemer levert hosting van ontwikkel, test, acceptatie, productie en educatie omgevingen (OTAPE) omgevingen met backup en restore faciliteiten (en een Uitwijk omgeving indien nodig voor continuiteit), conform de niet-functionele eisen.
NF-45	Hosting	De omgevingen zijn schaalbaar. De A en P omgeving kunnen initieel 50TB aan data kunnen bevatten en de O, T en E omgevingen 1 TB aan data (exclusief backup).
NF-46	Hosting	Opdrachtnemer realiseert adequate, beveiligde en redundante verbindingen tussen de Oplossing en het SVB netwerk waardoor beveiliging, beschikbaarheid en performance conform de niet-functionele eisen, gegarandeerd wordt.
NF-47	Hosting	Opdrachtnemer legt in het technisch ontwerp van de Oplossing de architectuur van de verbindingen vast, conform de niet-functionele eisen.
NF-48	Hosting	Opdrachtnemer realiseert integratie van alle omgevingen (OTAPE) met de SVB identity management oplossing, incl. analyse, ontwerp en testen (incl. testrapportage).
NF-49	Hosting	Opdrachtnemer realiseert integratie van alle omgevingen (OTAPE) met het SVB OpenShift integratie platform voor interfacing. Incl. analyse, ontwerp en testen (incl. testrapportage).
NF-50	Hosting	Opdrachtnemer realiseert integratie van alle omgevingen (OTAPE) met de SVB mail functionaliteit. Incl. analyse, ontwerp en testen (incl. testrapportage).
NF-51	Implementatie	Opdrachtnemer stelt vóór de start van de implementatie in overleg met de SVB een Projectplan op ter goedkeuring en vaststelling door de SVB
NF-52	Implementatie	Opdrachtnemer voert een analyse van de benodigde systeem configuratie uit ten behoeve van de inrichting van de Oplossing op basis van de eisen en wensen van SVB, conform functionele en niet-functionele eisen.
NF-53	Implementatie	Opdrachtnemer legt de configuratie van de Oplossing systeem configuratie vast in ontwerp documentatie (incl. access layers, rollen, rechten, metadata) conform de functionele en niet-functionele eisen.

NF-54	Implementatie	Opdrachtnemer voert de configuratie van de Oplossing uit op alle omgevingen (OTAPE), conform de functionele en niet-functionele eisen.
NF-55	Implementatie	Opdrachtnemer voert in overleg met de SVB testen van de configuratie van de Oplossing uit, incl. testplan en rapportage.
NF-56	Implementatie	Opdrachtnemer voert met de SVB analyse van de interfaces met de Oplossing uit. Dit betreft de volgende interfaces: • De SVB identity management oplossing • Het SVB OpenShift integratie platform • De SVB mail functionaliteit • Het SVB dataplatform
NF-57	Implementatie	Opdrachtnemer legt het ontwerp van de interfaces met de Oplossing vast in ontwerp documentatie, conform de niet-functionele eisen. Dit betreft de volgende interfaces: • De SVB identity management oplossing • Het SVB OpenShift integratie platform • De SVB mail functionaliteit • Het SVB dataplatform
NF-58	Implementatie	Opdrachtnemer realiseert in samenwerking met de SVB de interfaces, conform de niet-functionele eisen. Dit betreft de volgende interfaces: • De SVB identity management oplossing • Het SVB OpenShift integratie platform • De SVB mail functionaliteit • Het SVB dataplatform
NF-59	Implementatie	Opdrachtnemer voert in samenwerking met de SVB testen van de interfaces met de Oplossing uit, incl. testplan en rapportage. Dit betreft de volgende interfaces: • De SVB identity management oplossing • Het SVB OpenShift integratie platform • De SVB mail functionaliteit • Het SVB dataplatform
NF-60	Infrastructurele beveiligingseisen	De Oplossing dient te voldoen aan het ‘Defense in depth’ concept door de inrichting van meerdere beveiligingslagen en/of maatregelen (lees toegepaste preventieve, detectieve en/of correctieve maatregelen).
NF-61	Infrastructurele beveiligingseisen	De Oplossing moet alleen toegankelijk zijn via door de SVB goedgekeurde endpoints.
NF-62	Licenties	De Opdrachtnemer levert het gebruiksrecht (licentie) voor het gebruik van de oplossing voor ontwikkel, test, acceptatie, productie en educatie omgevingen (OTAPE), en een uitwijk omgeving indien nodig voor continuiteit.

NF-63	Licenties	Opdrachtnemer draagt zorg voor het beheer, onderhoud en vernieuwing van de Oplossing zodat deze technisch, functioneel en aan de voor de SVB geldende wet- en regelgeving blijft voldoen.
NF-64	Licenties	Opdrachtnemer stelt 20 beheer accounts per omgeving (OTAPE) beschikbaar.
NF-65	Licenties	Opdrachtnemer stelt 30 API accounts per omgeving (OTAPE) beschikbaar.
NF-66	Logische toegangsbeveiliging	Opdrachtnemer moet de SVB in staat stellen om aan te tonen dat er betrouwbare, effectieve en controleerbare mechanismen zijn voor het vastleggen en vaststellen van de identiteit van gebruikers en het toekennen van rechten aan gebruikers bij het gebruik van de Oplossing (i.h.k.v. de gevraagde dienstverlening) door gebruikers.
NF-67	Logische toegangsbeveiliging	Opdrachtnemer dient conform afspraken in de Overeenkomst de toegangsrechten van zijn medewerkers die werkzaamheden uitvoeren ten behoeve van de gevraagde dienstverlening te controleren (SOLL / IST vergelijking) en eventuele afwijkingen onmiddellijk te corrigeren.
NF-68	Logische toegangsbeveiliging	In het kader van rollen en functiescheiding moet voor de gewenste dienstverlening voldoende granulariteit mogelijk zijn om afscherming van gegevenssets zodanig in te richten, dat alleen gegevens die noodzakelijk zijn (autorisatie principes ‘least privilege’, ‘need-to-know’, ‘need-to-use’ en ‘Separation of duties’) voor de uitvoering van de werkzaamheden, beheertaken e/o speciale bevoegdheden toegankelijk zijn voor herleidbaar geautoriseerde gebruikers. Opdrachtnemer mag in het kader van de gevraagde dienstverlening alleen door de SVB goedgekeurde autorisatiematrices implementeren.
NF-69	Migratie	Opdrachtnemer voert in overleg met de SVB een analyse uit ter voorbereiding van de data migratie vanuit het SVB legacy systeem naar de Oplossing.
NF-70	Migratie	Opdrachtnemer stelt in overleg met de SVB een data migratie plan op voor de migratie van data uit het SVB legacy systeem naar de Oplossing.
NF-71	Migratie	Opdrachtnemer stelt in overleg met de SVB een data migratie ontwerp op waarin de export specificatie, data mapping en import specificatie beschreven staan. Binnen de Oplossing moeten de legacy unieke identifiers van geïmporteerde informatieobjecten bruikbaar zijn.
NF-72	Migratie	Opdrachtnemer voert de export van data uit het SVB legacy systeem uit, inclusief validatie van data op de ontwikkel, test, acceptatie, productie en educatie omgevingen, inclusief test rapportages. De migratie op de Productie omgeving betreft ± 200 miljoen informatieobjecten en 42TB aan data. Opdrachtnemer levert de benodigde tooling en omgevingen voor de migratie en het testen daarvan.
NF-73	Migratie	Opdrachtnemer voert de import van legacy data in de Oplossing uit, inclusief validatie van data op de ontwikkel, test, acceptatie, productie en educatie omgevingen en test rapportages. De migratie op de Productie omgeving betreft ± 200 miljoen informatieobjecten en 42TB aan data. Opdrachtnemer levert de benodigde tooling en omgevingen voor de migratie en het testen daarvan.
NF-74	Migratie	Van geïmporteerde informatieobjecten moeten de unieke identifiers vanuit het legacy systeem bruikbaar zijn in de Oplossing.

NF-75	Migratie	Opdrachtnemer stelt een testplan op en voert testen uit van de data migratie uit op de op de ontwikkel, test, acceptatie, productie en educatie omgevingen, incl. test rapportage.
NF-76	Migratie	Opdrachtnemer levert de benodigde tooling en omgevingen voor de migratie en het testen daarvan.
NF-77	Ontwikkelen en deployen	De ontwikkel-, test-, acceptatie en educatie omgevingen zijn logisch gescheiden van de productie omgeving.
NF-78	Ontwikkelen en deployen	Bij het ontwikkelen, testen, accepteren, educeren van de bedrijfsprocessen in de Oplossing kan de SVB gebruik maken van test data uit de corresponderende O-T-A-E omgevingen van de diverse aanleverende en afnemende systemen.
NF-79	Overleg & rapportage	Opdrachtnemer moet zorg dragen voor een periodieke rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen (incl. privacy) en het gerealiseerde beveiligingsniveau (BIO-compliance niveau BBN2), daartoe moet periodiek gestructureerd overleg plaatsvinden om issues en rapportages (comply or explain) te bespreken over de gevraagde dienstverlening met de volgende onderwerpen: • Onderkende risico's inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen • Security hardening proces inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen • Vulnerability management proces inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen • Lifecycle & patchmanagement proces inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen • Uitgevoerde penetratietesten inclusief de status van de opvolging /afhandeling van geconstateerde bevindingen • Loggings- en detectie-informatie monitoringsbevindingen van ICT-Componenten en de status van de opvolging /afhandeling van geconstateerde bevindingen • Resultaten van de periodieke controle van de toegangsrechten van de eigen medewerkers die werkzaamheden uitvoeren ten behoeve van de gevraagde dienstverlening.
NF-80	Overleg & rapportage	Opdrachtnemer draagt in het kader van de gevraagde dienstverlening jaarlijks zorg voor inzicht (in overleg e/o in rapportage) in onderstaande onderwerpen: • Overzicht van afwijkingen ten opzichte van beleid en onze overeenkomsten (contracten) • Onafhankelijke certificeringen en assurance verklaringen die past bij de aard van de gevraagde dienstverlening waarmee de opzet bestaan en werking van het passende stelsel aan beveiligings- en privacy maatregelen wordt aangetoond.
NF-81	Patch management	Opdrachtnemer borgt dat alle bij de oplossing betrokken ICT-Componenten zijn voorzien van de meest recente (beveiligings)patches en updates en zorgt dat installatie daarvan geen afbreuk doet aan de continuïteit en beschikbaarheid van de Oplossing. Installatie vindt plaats in overleg met de SVB.

NF-82	Penetratietesten	De SVB heeft het recht om een pentest uit te laten voeren om de beveiliging te testen in het kader van de gevraagde dienstverlening. De SVB kiest hierbij zelf een onafhankelijk en algemeen erkend bureau dat de testen uitvoert. De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
NF-83	Penetratietesten	Opdrachtnemer heeft een procedure om bij significante wijzigingen (bijvoorbeeld in gebruikname nieuwe dienst/ICT componenten) in het kader van de gevraagde dienstverlening af te wegen of deze wijziging moet worden onderworpen aan een pentest. De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
NF-84	Performance	Het aantal concurrent users is op en af te schalen.
NF-85	Performance (SLA)	De functionaliteit op de ontwikkel, test en educatie omgevingen van de Oplossing ondersteunt ten minste 10 concurrent users (beheerders) alsmede 5000 API aanroepen per uur, met een snelheid van gemiddeld minder dan 250ms per transactie, met dezelfde performance als voor de productie omgeving.
NF-86	Performance (SLA)	De acceptatie en productie omgeving van de Oplossing moet voldoende schaalbaar en performant zijn dat deze piekmomenten tot 20 concurrent users kan opvangen alsmede 200.000 API aanroepen per uur, met een snelheid van gemiddeld minder dan 250ms per transactie, tegen gelijkblijvende performance in overeenstemming met SLA.
NF-87	Performance (SLA)	De Oplossing moeten schaalbaar zijn, zowel wat betreft het aantal opgeslagen objecten als het beschikbare opslagvolume, met een mogelijkheid om extra opslag toe te voegen en opslag te verminderen. de Oplossing moet het volgende ondersteunen: • De huidige DMS data (Apr 2023) is 37 TB DMS en 65TB backup data. 190 miljoen documenten. Groei per maand is momenteel 0.7%. Deze aantallen kunnen groeien of krimpen in de toekomst • De mogelijkheid om uit te breiden tot ten minste een miljard documenten en een petabyte aan inhoud in totaal, indien nodig met behulp van meerdere repositories.
NF-88	Performance (SLA)	De Oplossing heeft geen beperkingen betreffende het aantal te creëren interfaces. Bij initiële implementatie zijn er ongeveer 20 bedrijfssytemen welke via het generieke koppelvlak zullen interfacen met de Oplossing.
NF-89	Performance (SLA)	Batchverwerking (via de API's) door middel van functionaliteit binnen de Oplossing mag de performance van de Oplossing voor andere Eindgebruikers niet negatief beinvloeden.
NF-90	Privacy	De Opdrachtnemer dient de SVB op verzoek te allen tijde te ondersteunen bij de uitoefening van de rechten van betrokkenen (AVG) en/of de opvolging of afhandeling van datalekken.
NF-91	Privacy	Opdrachtnemer zal de van de SVB ontvangen persoonsgegevens uitsluitend op basis van schriftelijke instructies van de SVB verwerken voor doeleinden die rechtstreeks voortvloeien uit de werkzaamheden die partijen zijn overeenkomen, en Opdrachtnemer zal de persoonsgegevens dus niet gebruiken voor: • Het uitvoeren van testen • Het uitvoeren van data-analyses

NF-92	Privacy	De Opdrachtnemer heeft met alle Onderaannemers in het kader van de gevraagde dienstverlening een verwerkersovereenkomst met hierin een clausule informatiebeveiliging/geheimhouding.
NF-93	Privacy	Tijdelijke bestanden e/o logs met betrekking tot de Oplossing moet zo min mogelijk persoonsgegevens bevatten in de productie omgeving. Opdrachtnemer dient dit periodiek te evalueren. Een BSN mag in ieder geval nooit in logbestanden van Opdrachtnemer voor komen. Deze tijdelijke bestanden e/o logbestanden dienen minimaal 15 maanden bewaard te worden.
NF-94	Rapportage	De Oplossing biedt de mogelijkheid tot het exporteren van metadata-objecten met de bijbehorende metadata en informatieobjecten naar een analyse & rapportage omgeving.
NF-95	Rapportage	Opdrachtnemer zorgt voor facturen waarop de aantallen van de afgenomen producten en diensten gespecificeerd zijn
NF-96	Rapportage (SLA)	Opdrachtnemer geeft periodiek inzicht (ten minste éénmaal per maand) in de geleverde prestaties, dmv een SLA rapportage op de afgesproken KPI's.
NF-97	Rapportage (SLA)	Bij het niet halen van de afgesproken service levels van de Oplossing en/of dienstverlening, start Opdrachtnemer onverwijld een onderzoek naar de oorzaak daarvan en rapporteert zij schriftelijk hierover aan de SVB. Dat rapport moet ook een (voorlopig) plan voor verbetering en planning daarvan bevatten. Opdrachtnemer moet steeds het initiatief nemen om een bespreking van dat rapport te plannen met de SVB en voor te zitten.
NF-98	Rapportage (SLA)	Opdrachtnemer moet periodiek (ten minste éénmaal per kwartaal) rapporteren over de voortgang van de realisatie van alle eventuele verbeterplannen
NF-99	Rapportage (SLA)	De Opdrachtnemer verplicht zich tot verbeteren/ vernieuwen / bijhouden van de Oplossing naar aanleiding van nieuwe of gewijzigde wet- en regelgeving en landelijke standaarden voor overheden zonder hiervoor extra kosten in rekening te brengen, en zorgt ervoor dat de Oplossing en de Dienstverlening te allen tijde in overeenstemming dient te zijn met de geldende wet- en regelgeving.
NF-100	Rapportage (SLA)	Indien nodig kunnen er op verzoek van de SVB aanvullende overleggen naast het maandelijks rapportage worden ingeregeld zoals: • Security overleg • Tactisch overleg • Strategisch overleg • Architectuur overleg
NF-101	Release management	Opdrachtnemer verplicht zich om tijdig correctief, perfectief, preventief, adaptief en vernieuwend onderhoud aan de Oplossing te plegen. De Opdrachtnemer verricht alle onderhoud op de Oplossing zonder daarvoor extra kosten in rekening te brengen (naast de overeengekomen vergoedingen voor het gebruik van de Oplossing en de Dienstverlening).
NF-102	Release management	De uitrol van updates en nieuwe releases van de Oplossing worden uitsluitend in overleg tussen SVB en Opdrachtnemer ingepland en uitgevoerd.

NF-103	Risico analyses	Opdrachtnemer heeft procedures om de analyse van risico's te borgen in het kader van de gevraagde Oplossing en Dienstverlening. De (opvolging van de) voor de SVB relevante (Informatiebeveiligings)-risico's en mitigerende maatregelen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
NF-104	Security Hardening	Security hardening moet procesmatig, ondersteund door gestandaardiseerde configuraties en vastgestelde richtlijnen (gebaseerd op internationaal erkende security hardening standaarden), worden uitgevoerd op alle ICT-systemen (zoals middelware, databases, platformen/infrastuctuur, netwerken, connectiviteit) van de Oplossing. De hardening wordt, getoetst, actueel gehouden en en de geconstateerde afwijkingen worden hersteld en meegenomen in de met de SVB afgesproken rapportagecyclus.
NF-105	Standaarden	De Oplossing ondersteunt Unicode Transformation Format (UTF) UTF-8 of UTF-16.
NF-106	Standaarden	Indien de Oplossing gebruik maakt van Microsoft (Azure), dient rekening gehouden te worden met maatregelen van de DPIA SLM Rijk - Microsoft: https://slmmicrosoftrijk.nl/wp-content/uploads/2022/02/Public-DPIA-Teams-OneDrive-SharePoint-and-Azure-AD-16-Feb-2022.pdf
NF-107	Standaarden	Indien de Oplossing gebruik maakt van Amazon AWS, dient Rekening gehouden te worden met maatregelen van de DPIA SLM Rijk - Amazon: https://slmmicrosoftrijk.nl/wp-content/uploads/2023/06/DPIA-AWS-EC2-S3-RDS-P-20230622.pdf
NF-108	Standaarden	Indien de Oplossing gebruik maakt van Google Cloud, dient rekening gehouden te worden met maatregelen van de DPIA SLM Rijk - Google: https://slmmicrosoftrijk.nl/wp-content/uploads/2021/03/Google-Workspace-DPIA-for-Dutch-DPA-v18-Feb-2021.pdf
NF-109	Standaarden	De Oplossing biedt een mogelijkheid om metadata-objecten, relaties tussen metadataobjecten en informatieobjecten zonder onredelijke inspanningen in een gestructureerd en gangbaar bestandsformaat te importeren vanuit het SVB IBM Content Manager systeem en vanuit andere Document Management of Content Services Platform systemen naar de Oplossing van Opdrachtnemer.
NF-110	Standaarden	Als bestandsformaat voor het importeren en exporteren van metadata-objecten met bijbehorende metadata moet tenminste het open standaard formaat CSV ondersteund worden.
NF-111	Standaarden	Export van dossiers, informatieobjecten en metadata voor overbrenging naar het e-depot van het Nationaal Archief moet in het formaat van het Nationaal Archief voor de overheidsgegevensuitwisseling zijn. Op korte termijn is dit MDTO, op lange termijn zullen dit opvolgers zijn.
NF-112	Standaarden	Indien de Oplossing gebruik maakt van een eigen gebruikersadministratie, dan ondersteunt deze out-of-the-box geautomatiseerde user provisioning zodat door SVB geautoriseerde gebruikers via een Koppeling met het identity management systeem van de SVB (op dit moment Azure AD voor cloud oplossingen) geautomatiseerd kunnen worden aangemaakt, geautoriseerd, gemuteerd en verwijderd/gearchiveerd.

NF-113	Standaarden	De Oplossing biedt een directe mailfunctionaliteit m.b.v. het SMTP protocol met ondersteuning van Modern Authentication.
NF-114	Standaarden	Koppelingen tussen SaaS oplossingen mogen alleen rechtstreeks gelegd worden als er sprake is van een bewezen standaard beschikbare koppeling die als onderdeel van de standaard SaaS oplossing worden aangeboden door beide Opdrachtnemers. Hiervan moet bewijs worden aangeleverd ten tijde van de aanbesteding. Bewijs kan geleverd worden door beide Opdrachtnemers middels documentatie over standaard connectoren voor koppeling tussen beide systemen en de informatie die uitgewisseld kan worden via de connectoren. Alternatief: Als de standaard beschikbare koppeling niet bewezen kan worden, moet de koppeling via het integratieplatform van SVB worden geïmplementeerd volgens de integratiepatronen van de SVB ten behoeve interoperabiliteit.
NF-115	Standaarden	De Oplossing moet Create-Read-Update-Delete (CRUD) functies ondersteunen via interfaces (API's).
NF-116	Standaarden	De Oplossing gebruikt de voorkeursstandaard REST/JSON web services of opvolgers hiervan voor de koppeling van gebruikende applicaties.
NF-117	Standaarden	Voor REST API koppelingen moet de open standaard OpenAPI Specification (OAS) voor het specificeren van de API gebruikt worden. Zie: https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification.
NF-118	Standaarden	API's moeten een versiebeleid hebben.
NF-119	Standaarden	Koppelingen die van belang zijn voor de Oplossing en in beheer zijn bij Opdrachtnemer (of toeleveranciers van Opdrachtnemer) hebben specificaties (descriptor documents). Voor elke koppeling met een interne of externe applicatie wordt minimaal het volgende beschreven: • Functie(s) • Wijze toegang • Aanroep • Berichtsoorten en -inhoud • Technische limieten
NF-120	Standaarden	Voor REST API koppelingen moeten de volgende verplichte open standaard REST-API Design Rules gebruikt worden voor het documenteren van de API. Zie: https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules.
NF-121	Standaarden	De Oplossing moet een periodieke batchgewijze verwerking kunnen ondersteunen.
NF-122	Standaarden	De Oplossing dient elke koppeling tussen applicaties / services en ICT-componenten in te richten op basis van algemeen geaccepteerde standaarden waarbij uitwisselingen tussen verschillende security domeinen verloopt via gedefinieerde koppelpunten van de SVB.
NF-123	Standaarden	De Oplossing biedt Multi Repository support ter ondersteuning van meerdere logisch danwel fysiek gescheiden repositories.

NF-124	Standaarden	Opdrachtnemer zorgt dat alle (maatwerk- en standaard) koppelingen die van belang zijn voor de Oplossing en in beheer zijn bij Opdrachtnemer (of toeleveranciers van Opdrachtnemer) blijven werken bij nieuwe releases en upgrades van de Oplossing. Deze Koppelingen maken tevens deel uit van het informatiebeveiligingsbeleid van Opdrachtnemer en vallen binnen de scope van de SLA.
NF-125	Standaarden	Koppelingen die van belang zijn voor de Oplossing en in Beheer zijn bij Opdrachtnemer (of toeleveranciers van de SVB) stellen de SVB in staat om ten aanzien van de A en P-omgeving near-realtime data uit te wisselen.
NF-126	Systeembeheer	De Oplossing biedt een dashboard waarin de technische status van de Oplossing en gesignaleerde foutsituaties zijn af te lezen.
NF-127	Tracking en tracing / logging	De Opdrachtnemer dient de log-events met betrekking tot het gedrag van de (SVB-)gebruikers en de toegang en handeling op de SVB-data binnen die dienstverlening en/of applicatie beschikbaar te stellen aan de SVB. Dit middels een nader overeen te komen timing, gangbaar format (zoals .csv) en overdracht-mechanisme tussen de SVB en Opdrachtnemer waarbij een adequate bescherming van deze data wordt toegepast.
NF-128	Tracking en tracing / logging	De Oplossing dient transactie/ audit/ logbestanden minimaal 15 maanden te bewaren voor toekomstig onderzoek en toegangscontrole.
NF-129	Tracking en tracing / logging	Bij applicatiefouten tijdens gebruik van de Oplossing wordt een foutmelding gelogd en SVB Beheerders kunnen instellen van welke fouten ze een notificatie ontvangen.
NF-130	Tracking en tracing / logging	De audittrail van acties kan niet worden aangepast.
NF-131	Tracking en tracing / logging	Een foutmelding bevat voldoende informatie zodat SVB-Beheerders zelf fouten kunnen herstellen (bijvoorbeeld aanleiding, tijdstip, aard van de fout en context waarbinnen de fout is opgetreden).
NF-132	Tracking en tracing / logging	Van mutaties op records (dossiers, informatieobjecten) moet het mogelijk zijn de oude en de nieuwe waarde van de metadata in de audittrail vast te leggen.
NF-133	Tracking en tracing / logging	De Oplossing biedt rapportagemogelijkheden over hoe de SVB de Oplossing gebruikt. De Oplossing biedt ten minste statistieken over gebruikers, documenten en opslag.
NF-134	Tracking en tracing / logging	De Oplossing biedt de mogelijkheid om beperkingen toe te passen op bepaalde bestandtypes en bestandsformaten. Deze beperkingen zijn aan te passen door de de beheerder bij de SVB.
NF-135	Training	Opdrachtnemer stelt in overleg met de SVB een training plan op waarin beschreven wordt welke trainingen, in welke vorm en aan welke doelgroep gegeven worden.
NF-136	Training	Trainingen zijn in de Nederlandse of Engelse taal.
NF-137	Training	Opdrachtnemer levert een initiële training in de Oplossing voor 20 SVB IT beheerders/developers.
NF-138	Training	Opdrachtnemer levert een jaarlijkse training (bijscholing) in de Oplossing voor 20 SVB IT beheerders/developers.

NF-139	Vulnerability management	Opdrachtnemer heeft een procedure waar wordt geborgd dat continu naar nieuwe kwetsbaarheden en dreigingen wordt gezocht (vulnerability management) in het kader van regulier beheer en bij in gebruik name van een nieuwe dienst/ict-component/significante wijziging. De (opvolging van de) voor de SVB relevante bevindingen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
NF-140	Webapplicatie	Een geautoriseerde beheerder kan de Oplossing benaderen via een webbased applicatie (browser). De geleverde Oplossing dient qua standaarden en technische specificaties te voldoen aan de standaarden zoals opgesteld door het World Wide Web Consortium (W3C), dan wel de logische opvolgers daarvan.
NF-141	Webapplicatie	De Oplossing werkt naar behoren voor geautoriseerde beheerders voor zover zij gebruik maken van de standaardinrichting van een werkstation binnen de SVB. Dit houdt onder meer in dat er geen aanvullende software of scripts vereist zijn voor het gebruik van de Oplossing.
NF-142	Webapplicatie	De presentatielaag van de Oplossing (browser) functioneert met minimaal de laatste twee versies van: • Google Chrome; • Microsoft Edge; En moet marktconforme browsers ondersteunen (Marktconform als het een aandeel heeft van 5% van de markt, volgens W3.org, of de natuurlijke opvolger is van een bestaande marktconforme browser)
NF-143	Webapplicatie	De presentatielaag van de Oplossing functioneert zonder aanvullende proprietary plugins of extensies.
NF-144	Webapplicatie	De Oplossing is gebruikersvriendelijk voor beheerders. Dit houdt ten minste in dat het aantal handelingen dat nodig is om een taak uit te voeren zo beperkt mogelijk is, dat de user interface overzichtelijk is, dat de user interface en de user experience intuïtief zijn en beperkte training vereisen, dat er een eenvoudig en snelle zoekfunctie beschikbaar is voor gebruikers waarmee informatie en functies eenvoudig vindbaar zijn.
NF-145	Webapplicatie	Voor de gevraagde dienstverlening moet de Oplossing van Opdrachtnemer, en koppelingen die daarvoor van belang zijn, persoonsgegevens in opslag (at rest) e/o in transport (in transit) versleutelen waarbij minimaal moet worden voldaan aan de cryptografische beveiligingsvoorzieningen zoals voorgeschreven in de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS). Momenteel TLS1.2 of hoger. https://www.ncsc.nl/onderwerpen/verbindingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
NF-146	Webapplicatie	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid zodat de Oplossing voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.
NF-147	Webapplicatie	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid om de op basis van de OWASP top tien (https://owasp.org/www-project-top-ten/) meest kritische beveiligingsrisico’s binnen een webapplicatie te vermijden voor wat betreft de Oplossing.