

Nummer	Hoofdcategorie	Subcategorie	Als	wil ik	zodat
F-E01	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	Content kunnen uploaden en delen met de gehele organisatie	het zichtbaar en bruikbaar is voor de Lerende.
F-E02	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	zelfstudiemodules, zoals GoodHabit, kunnen uploaden, al dan niet met behulp van een LTI-koppeling	het zichtbaar en bruikbaar is voor de Lerende.
F-E03	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	bestanden van diverse formaten (zoals video en audio formats) kunnen uploaden	een Lerende deze bestanden tot zich kan nemen.
F-E04	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	bestanden kunnen voorzien van metadata	er in bestanden gezocht kan worden en analyses plaats kunnen vinden op basis van de metadata.
F-E05	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	Content beschikbaar kunnen stellen aan alle Gebruikers of specifieke Gebruikers (op basis van functie, locatie, etc.). Dit middels een automatische toewijzing, individuele inschrijving of groepsinschrijving	De juiste content voor de juiste Lerende beschikbaar is.
F-E06	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	Content kunnen updaten naar nieuwere versies	zodat de Lerende altijd de meest actuele content tot zijn of haar beschikking heeft.
F-E07	Content digitaal delen	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	Content ontoegankelijk kunnen maken zonder deze direct te verwijderen / archiveren	Lerenden geen toegang hebben tot de content, maar de inhoud niet verloren gaat.
F-E08	Content migratie	Migratie	Content ontwikkelaar / beheerder	dat de bestaande Content, vragenbank (bibliotheek) en toetsmatrijs in Moodle gemigreerd worden naar het LES	zodat dit straks hergebruikt kan worden in het LES en niet opnieuw ontwikkeld hoeft te worden.
F-E09	Content migratie	Migratie	Lerende	dat bestaande HR data (POB, certificaten, historie Leeractiviteiten, actuele Leeractiviteiten) worden gemigreerd naar het LES	zodat mijn persoonlijke data behouden, inzichtelijk en aantoonbaar blijft.
F-E10	Content digitaal delen	Waarderen	Lerende	afgeronde Leerinterventies kunnen beoordelen met sterren/punten en tekst.	ik kan anderen inzicht kan geven in de kwaliteit en de kwaliteit van Leerinterventies geborgd is.

F-E11	Content digitaal delen	Waarderen	Lerende	een review kunnen toevoegen over Leerinterventies die ik heb gevolgd	ik kan anderen inzicht kan geven in de kwaliteit en de kwaliteit van Leerinterventies geborgd is.
F-E12	Content digitaal delen	Waarderen	Backoffice medewerker	gedane reviews kunnen modereren	er geen ongewenste (bv. in verband met ongepast taalgebruik) reviews zichtbaar blijven bij Leerinterventies.
F-E13	Content digitaal delen	Waarderen	Content ontwikkelaar / beheerder	gebruik kunnen maken van psychologische beloningsstrategieën t.a.v. het leren (Gamification)	leren gestimuleerd kan worden door middel van incentives.
F-E14	Leerervaring maken	Interactieve zelfstudiecontent maken	Content ontwikkelaar / beheerder	interactieve Content kunnen maken	Lerenden gestimuleerd kunnen worden om actief te leren in plaats van passief.
F-E15	Leerervaring maken	Interactieve zelfstudiecontent maken	Content ontwikkelaar / beheerder	interactieve Content kunnen publiceren	Lerenden daadwerkelijk gebruik kunnen maken van de interactieve Content.
F-E16	Leerervaring maken	Interactieve zelfstudiecontent maken	Content ontwikkelaar / beheerder	interactieve Content kunnen aanpassen	Lerenden altijd beschikking hebben over de meest actuele en juiste versie van de Content.
F-E17	Leerervaring maken	Interactieve zelfstudiecontent maken	Content ontwikkelaar / beheerder	interactieve Content kunnen downloaden	ik de Content kan hergebruiken voor andere doeleinden.
F-E18	Leerervaring maken	Interactieve zelfstudiecontent maken	Content ontwikkelaar / beheerder	alle Content kunnen delen in verschillende Leerinterventies	de Content op één plaats beheerd kan worden en de juiste versie altijd inzichtelijk is in de verschillende Leerinterventies.
F-E19	Leerervaring maken	Toetsen maken	Content ontwikkelaar / beheerder	verschillende vraagsoorten kunnen toevoegen aan toetsen	Lerenden op verschillende wijzen getoetst kunnen worden op bekwaamheid.
F-E20	Leerervaring maken	Toetsen maken	Content ontwikkelaar / beheerder	multimedia kunnen toevoegen aan toetsen	Lerenden op verschillende wijzen getoetst kunnen worden op bekwaamheid.
F-E21	Leerervaring maken	Toetsen maken	Content ontwikkelaar / beheerder	restricties (zoals tijdvak of aantal pogingen) kunnen instellen voor toetsen	de toets kan voldoen aan de criteria die daarvoor zijn gesteld.
F-E22	Leerervaring maken	Toetsen maken	Content ontwikkelaar / beheerder	de validiteit en betrouwbaarheid van toetsen kunnen analyseren	de kwaliteit van toetsen verbeterd kan worden.

F-E23	Leerervaring maken	Toetsen maken	Lerende	kunnen beschikken over uitgebreide feedback mogelijkheden t.a.v. toetsen	ik eventuele opmerkingen over de betreffende toets kan terugkoppelen aan de trainer of maker van de toets.
F-E24	Leren	Inschrijving & autorisatie	Lerende	mij kunnen inschrijven (of laten inschrijven) voor een Leerinterventie in het LMS, waarbij ik vervolgens direct in de leeromgeving (ELO) terecht kom	ik direct aan de slag kan met de Leerinterventie naar keuze.
F-E25	Leren	Leerinterventies opstellen/samenstellen	Content ontwikkelaar / beheerder	een cursus kunnen aanmaken	we deze vervolgens beschikbaar kunnen stellen aan de Lerenden.
F-E26	Leren	Leerinterventies opstellen/samenstellen	Content ontwikkelaar / beheerder	een cursus kunnen koppelen aan een Catalogusitem, zoals een thema, en eventuele uitvoeringen/bijeenkomsten	deze gecategoriseerd kunnen worden en vervolgens ook daadwerkelijk gevonden.
F-E27	Leren	Leerinterventies opstellen/samenstellen	Content ontwikkelaar / beheerder	een cursus kunnen openstellen en/of publiceren	deze gevolgd kan worden door de Lerenden.
F-E28	Leren	Leerinterventies opstellen/samenstellen	Content ontwikkelaar / beheerder	eventueel cursussen kunnen combineren in een curriculum	verplichte cursussen kunnen worden samengevoegd tot één curriculum.
F-E29	Leren	Leerpaden samenstellen	Content ontwikkelaar / beheerder	Leerpaden kunnen aanmaken	deze gevolgd kunnen worden door de Lerenden.
F-E30	Leren	Leerpaden samenstellen	Content ontwikkelaar / beheerder	groepsinschrijvingen op leerpaden/programma's mogelijk kunnen maken (bulkinschrijving / toewijzingsprofiel)	grotere groepen Lerenden gezamenlijk en snel ingeschreven kunnen worden.
F-E31	Leren	Leerpaden samenstellen	Content ontwikkelaar / beheerder	zowel Leerinterventies, Content en activiteiten kunnen combineren tot Leerpaden	ik Leerpaden kan opstellen die vervolgens aangeboden kunnen worden aan de lerenden.
F-E32	Leren	Leerpaden samenstellen	Content ontwikkelaar / beheerder	Leerpaden kunnen onderbrengen in thema's, kanalen en tracks	Leerpaden op de juiste wijze kunnen worden gecategoriseerd en aangeboden.
F-E33	Leren	Leerpaden samenstellen	Content ontwikkelaar / beheerder	Leerpaden kunnen publiceren	deze daadwerkelijk gevolgd kunnen worden door de lerenden.
F-E34	Leren	Individueel leren	Lerende	een Leeractiviteit naar keuze kunnen opstarten op een moment naar keuze	ik kan leren wanneer dat mij uitkomt.

F-E35	Leren	Individueel leren	Content ontwikkelaar / beheerder	voorwaardelijk leren mogelijk maken (adaptief door mogelijkheid om specifieke Content te ontsluiten op basis van regels)	ik persoonlijk leren mogelijk kan maken, door bijvoorbeeld specifieke Content aan te bieden aan Lerenden met een bepaald profiel.
F-E36	Leren	Samen leren (social learning)	Content ontwikkelaar / beheerder	bijdrages enkel zichtbaar kunnen maken voor deelnemers in dezelfde groep	alleen groepsleden beschikking hebben over de inhoud die voor hen relevant is.
F-E37	Leren	Samen leren (social learning)	Content ontwikkelaar / beheerder	een docent, coach, begeleider of manager kunnen koppelen aan een specifieke groep en/of uitvoering	deze de groep op een juiste wijze kan meenemen in de leerervaring.
F-E38	Leren	Samen leren (social learning)	Lerende	asynchroon kunnen communiceren binnen een specifieke groep	ik kan communiceren wanneer dat mij uitkomt.
F-E39	Leren	Samen leren (social learning)	Lerende	opdrachten kunnen indienen bij een docent, die het kan voorzien van feedback	ik hiervan kan leren.
F-E40	Leren	Samen leren (social learning)	Lerende	gebruik kunnen maken van peer to peer feedback	we mét en van elkaar kunnen leren.
F-E41	Leren	Samen leren (social learning)	Lerende	content kunnen uploaden en delen met anderen binnen een groep	we mét en van elkaar kunnen leren.
F-E42	Leren	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	externe Leerinterventies en/of bronnen kunnen ontsluiten middels LTI	deze kunnen worden aangeboden aan de lerenden.
F-E43	Leren	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	Content van diverse bestandstypen kunnen insluiten op vele verschillende plekken en manieren (waaronder embedden) in het LES vanuit vele verschillende bronnen, zoals Vimeo en Microsoft 365	we deze content flexibel kunnen aanbieden aan de lerenden.
F-E44	Leren	Content toevoegen en/of beheren	Content ontwikkelaar / beheerder	een bron vanuit één locatie (bibliotheek) kunnen gebruiken voor verschillende Leerinterventies, waarbij ik kan kiezen voor het kopiëren van Content of het gebruiken van een alias/interne verwijzing (waarbij er maar één bronbestand blijft bestaan)	ik het beheer van deze Leerinterventies maar op één plaats hoeft uit te voeren i.p.v. dezelfde handelingen uitvoeren in diverse Leerinterventies waar dezelfde Content wordt ingezet.

F-E45	Leren	Toetsen afnemen	Content ontwikkelaar / beheerder	toetsen aan een individu of groep kan openstellen	deze daadwerkelijk de toets kunnen maken.
F-E46	Leren	Toetsen afnemen	Content ontwikkelaar / beheerder	een toets onder gecontroleerde omstandigheden (bv. een tijdslot) kan laten afnemen	een Lerende onder tijdsdruk op parate kennis getoetst kan worden.
F-E47	Leren	Toetsen afnemen	Lerende	een toets kunnen afbreken en op een later moment hervatten	ik een toets kan afleggen wanneer het mij uitkomt.
F-E48	Leren	Certificeren	Content ontwikkelaar / beheerder	een certificering kunnen koppelen aan een Leerinterventie	een Lerende beloond kan worden en zij aantoonbaar kunnen maken dat ze een Leerinterventie succesvol hebben afgerond.
F-E49	Leren	Certificeren	Content ontwikkelaar / beheerder	het mogelijk maken om een certificaat uit te reiken door een bepaalde rol (bijvoorbeeld trainer)	indien benodigd, een certificaat handmatig kan worden uitgereikt op initiatief van de persoon in deze rol.
F-E50	Leren	Certificeren	Content ontwikkelaar / beheerder	het mogelijk maken om een certificaat automatisch te laten uitreiken wanneer aan bepaalde voorwaarden is voldaan	een certificaat niet handmatig hoeft te worden uitgereikt.
F-E51	Leren	Certificeren	Content ontwikkelaar / beheerder	een geldigheidsduur kunnen koppelen aan een certificaat	het duidelijk is wanneer een certificaat niet langer geldig is en deze eventueel opnieuw behaald zal moeten worden.
F-E52	Leren	Certificeren	Content ontwikkelaar / beheerder	dynamische velden kunnen toevoegen aan een certificaat	ik flexibel kan zijn met het inrichten van een certificaat.
F-E53	Leren	Certificeren	Lerende	een certificaat kunnen downloaden en/of printen	ik deze eventueel elders kan aantonen.
F-E54	Leren	Tracken en tracen	SVB	dat de voortgang van Leeractiviteiten en leerobjecten geautomatiseerd kan worden vastgelegd (gestart, aantal keren bekeken, afgerond, etc.)	we op deze status kunnen monitoren en rapporteren.
F-E55	Leren	Tracken en tracen	SVB	dat Leeractiviteiten een status kunnen krijgen (nog niet gestart, bezig, afgerond, etc.)	we op deze status kunnen monitoren en rapporteren.
F-E56	Leren	Tracken en tracen	Lerende	een behaalde score mee kunnen krijgen op een Leeractiviteit	ik weet met welke score ik een Leeractiviteit heb afgerond.

F-E57	Leren	Tracken en tracen	SVB	dat een Leerinterventie een status "afgerond" krijgt gebaseerd op afgeronde Leeractiviteiten of andere criteria	we op deze status kunnen monitoren en rapporteren en de lerende aantoonbaar kan maken dat de Leerinterventie is afgerond.
F-E58	Leren	Tracken en tracen	SVB	dat een status kan worden ingediend door een bepaalde rol, zoals trainer	indien benodigd, de status handmatig kan worden doorgegeven.
F-E59	Leren	Rapportage	Lerende	inzicht hebben in de voortgang binnen Leerinterventies	ik weet in hoeverre ik de Leerinterventie heb afgerond
F-E60	Leren	Rapportage	Manager	voorgedefinieerde rapportages kunnen raadplegen	ik inzicht krijg in gegevens uit het LES
F-E61	Leren	Rapportage	Manager	rapportages geautomatiseerd opgestuurd kunnen krijgen	ik deze niet handmatig hoeft op te halen.
F-E62	Leren	Rapportage	Manager	dat het mogelijk is om zelf flexibele rapportages op te stellen	ik exact de gegevens inzichtelijk krijg waar ik behoefte aan heb.
F-E63	Leren	Communicatie	Lerende	automatische notificaties kunnen ontvangen	ik op de hoogte wordt gebracht van relevante updates.
F-E64	Leren	Communicatie	Lerende	individuele berichten kunnen sturen	ik kan communiceren met anderen, bijvoorbeeld trainers.
F-E65	Leren	Communicatie	Lerende	berichten aan een groep kunnen sturen	ik leren mét en van elkaar kan realiseren.
F-E66	Leren	Communicatie	Content ontwikkelaar / beheerder	het mogelijk maken om reminders geautomatiseerd kunnen sturen, gebaseerd op regels	medewerkers automatisch gewezen kunnen worden op zaken die voor hen relevant zijn.
F-E67	Data beheren	Analyseren van data	Functioneel Beheerder	queries kunnen gebruiken om data te onderzoeken	ik inzicht kan krijgen in de gegevens waar ik behoefte aan heb.
F-E68	Data beheren	Data ontsluiten	Functioneel Beheerder	data als input kunnen verwerken in andere systemen; bijvoorbeeld in zelfstudiemodules waarbij je gepersonaliseerde leerinhoud ziet zoals naam of functie	ik anderen inzicht kan geven in gegevens die alleen voor hen relevant zijn.
F-E69	Data beheren	Automatiseren acties	Content ontwikkelaar / beheerder	regels/toewijzingsprofielen ingesteld kunnen worden om handelingen te automatiseren	we mensen automatisch kunnen inschrijven / koppelen aan Leeractiviteiten wanneer dat noodzakelijk is.
F-E70	Leertrajecten beheren	Catalogus beheren	Lerende	de door de Broker gevulde Catalogus met intern en extern aanbod kunnen inzien	ik mij kan ontwikkelen middels het aanbod van de Broker.

F-E71	Leertrajecten beheren	Catalogus beheren	Leveranciersmanager SVB	dat delen van de Catalogus selectief opengesteld kunnen worden aan specifieke doelgroepen	zodat Gebruikers gemakkelijk een overzicht hebben van wat zij nodig hebben.
F-E72	Leertrajecten beheren	Catalogus beheren	Lerende	dat Catalogusonderdelen die tijdens de looptijd van de Overeenkomst zijn gearcheveerd, alsnog inzichtelijk zijn in mijn persoonlijke leerhistorie	zodat deze altijd aantoonbaar blijft.
F-E73	Leertrajecten beheren	Curricula en leerpaden maken	Content ontwikkelaar / beheerder	onderdelen uit de Catalogus kunnen combineren tot een curriculum en selectief kunnen openstellen aan bijvoorbeeld bepaalde doelgroepen	zodat Gebruikers gemakkelijk een overzicht hebben van wat zij nodig hebben.
F-E74	Leertrajecten beheren	Curricula en leerpaden maken	Content ontwikkelaar / beheerder	Leerpaden kunnen worden gemaakt en selectief worden opengesteld aan bijvoorbeeld bepaalde doelgroepen	zodat Gebruikers gemakkelijk een overzicht hebben van wat zij nodig hebben.
F-E75	Leertrajecten beheren	Curricula en leerpaden maken	Content ontwikkelaar / beheerder	opleidingsplannen kunnen maken en selectief openstellen aan bijvoorbeeld bepaalde doelgroepen	zodat Gebruikers gemakkelijk een overzicht hebben van wat zij nodig hebben.
F-E76	Leertrajecten beheren	Organisatiestructuur	Functioneel Beheerder	variabelen dynamisch kunnen inlezen vanuit andere SVB systemen (zoals rollen, functies, locatie, namen en personeelnummer)	deze binnen het LES kunnen worden gebruikt.
F-E77	Leertrajecten beheren	Organisatiestructuur	Functioneel Beheerder	dat mutaties in het bronsysteem ook direct nadat deze beschikbaar zijn gekomen, worden verwerkt	deze binnen het LES altijd up to date zijn.
F-E78	Leertrajecten beheren	Inschrijven & plannen	Content ontwikkelaar / beheerder	dat een deel van de Catalogus vrij toegankelijke Leerinterventies bevat waar deelnemers zich direct kunnen inschrijven	een Lerende met deze Leerinterventies direct kan starten.
F-E79	Leertrajecten beheren	Inschrijven & plannen	Content ontwikkelaar / beheerder	betalde Leerinterventies een goedkeuring vereisen van een leidinggevende, waarbij de mandateringsflow flexibel kan worden ingericht	een aanvraag conform de gehanteerde mandateringsflow goedgekeurd kan worden.

F-E80	Leertrajecten beheren	Inschrijven & plannen	Content ontwikkelaar / beheerder	dat elke stap in het inschrijfproces met een notificatie kan worden bevestigd	het voor de volgende persoon in de mandateringsflow duidelijk is dat er een actie van hem/haar wordt verwacht.
F-E81	Leertrajecten beheren	Inschrijven & plannen	Content ontwikkelaar / beheerder	notificaties op maat kunnen maken	we deze kunnen toespitsen op de specifieke situatie.
F-E82	Leertrajecten beheren	Inschrijven & plannen	Lerende	dat, bij een inschrijving met een maximaal aantal deelnemers, dit direct actueel inzichtelijk is voor de inschrijvers (en het aantal beschikbare plaatsen is zichtbaar)	ik weet of er nog voldoende plaats is om deel te nemen.
F-E83	Leertrajecten beheren	Proces van goedkeuring	Lerende	een opleidingsaanvraag kunnen indienen voor aanbod buiten de Catalogus	ik volledige vrijheid heb om de Leerinterventie te volgen die ik wil en het administratieve proces alsnog via het LeerEcoSysteem kan plaatsvinden.
F-E84	Leertrajecten beheren	Proces van goedkeuring	Lerende	dat een (persoonlijk) opleidingsbudget kan worden gekoppeld aan een individu, rol, functie of groep	ik altijd de stand van mijn persoonlijk opleidingsbudget inzichtelijk heb.
F-E85	Leertrajecten beheren	Proces van goedkeuring	Lerende	dat het persoonlijk opleidingsbudget wordt aangepast nadat er kosten zijn gemaakt	ik inzichtelijk heb wat de nieuwe stand is van mijn persoonlijk opleidingsbudget.
F-E86	Leertrajecten beheren	Inzicht resultaten & voortgang	Functioneel Beheerder	dat resultaten en learning data vanuit de leeromgeving zichtbaar zijn in het systeem	op deze gegevens gemonitord en gerapporteerd kan worden.
F-E87	Leertrajecten beheren	Resources beheren	Content ontwikkelaar / beheerder	interne resources kunnen worden toegevoegd, zoals lokalen, fysieke leermaterialen, docenten, coaches en apparatuur	deze meteen bij de Leerinterventie worden vastgelegd.
F-E88	Leertrajecten beheren	Resources beheren	Content ontwikkelaar / beheerder	resources kunnen aanpassen	eventuele wijzigingen kunnen worden toegepast.
F-E89	Leertrajecten beheren	Financieel beheren	SVB	actueel inzicht in alle investeringen rondom inkoop van Externe Leeractiviteiten	we kunnen monitoren op de gemaakte kosten.

F-E90	Leertrajecten beheren	Financieel beheren	SVB	persoonlijke opleidingsbudgetten op verschillende manieren kunnen inzetten en beheren	we deze flexibel kunnen inrichten op basis van gemaakte afspraken.
F-E91	Leertrajecten beheren	Financieel beheren	SVB	kostenposten kunnen inbrengen	we de financiële administratie op de juiste wijze kunnen laten verlopen.
F-E92	Leertrajecten beheren	Financieel beheren	SVB	kunnen doorbelasten naar afdelingen	we de financiële administratie op de juiste wijze kunnen laten verlopen.
F-E93	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat de Broker met nieuwe Aanbieders onderhandelt en contracten afsluit omtrent Externe Leeractiviteiten en daarmee tevens inkoopvoordeel realiseert voor de SVB	het aanbod voor de Lerenden altijd actueel en op orde is voor zo laag mogelijke kosten.
F-E94	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat de Broker contractbeheer en actualisatie uitvoert	het aanbod voor de Lerenden altijd actueel en op orde is.
F-E95	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat, bij vraag vanuit de SVB, de Broker helpt een match te vinden binnen de Catalogus (advies bieden)	de Lerende altijd de gewenste leerinterventie krijgt aangeboden.
F-E96	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat, bij vraag vanuit de SVB waarvoor geen passende Leeractiviteit in de Catalogus beschikbaar is, de Broker een nieuwe passende Leeractiviteit kan aanbieden	de Lerende altijd de gewenste Leerinterventie krijgt aangeboden.
F-E97	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat de Broker op aanvraag specifieke rapportages kan leveren	we altijd de gewenste gegevens inzichtelijk kunnen krijgen.
F-E98	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat de Broker het aanbod in de Catalogus actueel houdt	het aanbod voor de Lerenden altijd actueel en op orde is.
F-E99	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat de Broker verantwoordelijkheid neemt voor financieel beheer	we de financiële administratie op de juiste wijze kunnen laten verlopen.
F-E100	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat er een koppeling met het facturatiesysteem van de SVB wordt gerealiseerd	de ontvangen facturen automatisch door het facturatiesysteem Proactis ingelezen en verwerkt kunnen worden.

F-E101	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat de Broker fungeert als een intermediair (inclusief financieel administrateur) van een breed aanbod van opleidingen, bijvoorbeeld: - Trainingen; - Digitale leeractiviteiten; - Seminars / Congressen; - Assessments; - Online opleiders; - Coaches; - Inhuur van sprekers; - Adviseren over individuele aanvragen; - Begeleiden van individuele maatwerkaanvragen; - Operationele afhandeling van groepstrainingen op maat	Lerenden een keuze kunnen maken in alle gewenste opleidingssoorten.
F-E102	Brokerfunctionaliteit	Ondersteuning broker	SVB	volledige zeggenschap over welke Aanbieders wel of niet worden ontsloten en daarbij niet afhankelijk zijn van eventuele (financiële) afspraken tussen de Broker en Aanbieder	de SVB zelf kan bepalen welke Aanbieders wel/niet toe te laten.
F-E103	Brokerfunctionaliteit	Ondersteuning broker	SVB	de mogelijkheid hebben om de Broker in te zetten bij Maatwerk-aanvragen waarbij een transparante werkwijze wordt gehanteerd door de Broker en er geen sprake is van een voorkeur voor opleidingen uit het eigen aanbod	de Lerende altijd de gewenste Leerinterventie krijgt aangeboden.
F-E104	Brokerfunctionaliteit	Ondersteuning broker	SVB	vrij zijn om een voorkeur voor een uitvoerder aan te dragen bij een Maatwerkaanvraag en deze uitvoerder ook kunnen selecteren op basis van eigen argumentatie	de SVB zelf zeggenschap heeft over de te invulling van de Maatwerk-aanvraag.

F-E105	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat Interne en Externe Leeractiviteiten op dezelfde wijze worden aangeboden	de Gebruiker alle Leeractiviteiten op dezelfde wijze kan zoeken en vinden.
F-E106	Brokerfunctionaliteit	Ondersteuning broker	SVB	dat het aanbod van de Broker aansluit op de overige onderdelen uit het LES	het als één geheel kan worden aangeboden aan de Gebruikers.
F-E107	Brokerfunctionaliteit	Organisatiestructuur	Functioneel Beheerder	dat de organisatiestructuur en variabelen kunnen worden gebruikt door de Broker bij alle andere handelingen in het LES. Van openstellen van curricula t/m het gebruik van rapportages	de juiste mensen toegang hebben tot de benodigde functionaliteiten.

Nummer	Hoofdcategorie	Subcategorie	Non-functionele Eisen
NF-E1	Applicatieve eisen en wensen	Autorisatie gebruikers	De Oplossing kan overweg met Role Based Access Control (RBAC). In de Role claim worden alle rollen van de Gebruiker bij de Oplossing aangeboden. Wat betreft Role assignment wordt de rol van een Gebruiker aan een specifieke claim toegewezen die de Oplossing begrijpt.
NF-E2	Applicatieve eisen en wensen	Autorisatie gebruikers	De Oplossing en alle aanwezige data is beveiligd tegen ongeautoriseerde toegang.
NF-E3	Applicatieve eisen en wensen	Koppelingen	De Oplossing biedt een standaard functionaliteit om Gebruikers geautomatiseerd te autoriseren/ muteren/ verwijderen (en archiveren), middels een koppeling met het IAM van de SVB, op basis van SAML JIT, OIDC en/of SCIM2.0 of tenminste een API op basis van webtechnologie.
NF-E4	Applicatieve eisen en wensen	Koppelingen	Opdrachtnemer ondersteunt e-facturatie (in de huidige situatie in XML obv UBL 2.1).
NF-E5	Applicatieve Eisen en Wensen	Licenties	Opdrachtnemer levert alle softwarelicenties die nodig zijn voor de Dienstverlening en garandeert de SVB het ongestoorde gebruiksrecht gedurende de looptijd van de Overeenkomst.
NF-E6	Applicatieve Eisen en Wensen	Webapplicatie	De Oplossing is gebruikersvriendelijk. Dit houdt tenminste 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, en dat er een eenvoudig en snelle zoekfunctie beschikbaar is voor gebruikers waarmee informatie en functies eenvoudig vindbaar zijn. Deze gebruikersvriendelijkheid van de Oplossing wordt getoont in de Screencast opnames.
NF-E7	Architectuur	Autorisatie gebruikers	De Oplossing integreert met Azure AD SSO/MFA (QS Solutions) voor de authenticatie
NF-E8	Architectuur	Autorisatie gebruikers	De Oplossing integreert met SAML 2.0 of Oauth 2.0/OIDC 1.0. of WS-Federation v1.2
NF-E9	Architectuur	Koppeling Leersystemen	De Oplossing is SCORM compliant.
NF-E10	Architectuur	Licenties	De Oplossing is geschikt en volledig bruikbaar op flexplekken en thuiswerkplekken.
NF-E11	Architectuur	Webapplicatie	De presentatielaag van de Oplossing functioneert op minimaal de laatste twee softwareversies van Google Chrome, Microsoft Edge, Safari, Firefox, of nieuwe browsers die een marktaandeel van 5% of meer hebben of natuurlijke opvolgers zijn van de eerder genoemde browsers.
NF-E12	Architectuur	Webapplicatie	De presentatielaag van de Oplossing is webbased.
NF-E13	Architectuur	Webapplicatie	De presentatielaag van de Oplossing vereist geen installatie van eigen (propriety) software of scripts op het werkstation van een Gebruiker of Beheerder.
NF-E14	Architectuur	Webapplicatie	De presentatielaag van de Oplossing functioneert zonder aanvullende propriety plugins of extensies.
NF-E15	Business	Continuïteit	Opdrachtnemer heeft maatregelen getroffen om de downtime van de Dienstverlening te beperken tot maximaal 120 uur, ingeval van het eindigen van (cruciale delen van) de Dienstverlening als gevolg van faillissement (van Opdrachtnemer of diens onderaannemer) door onvoorziene omstandigheden of calamiteiten.
NF-E16	Business	Performance	Minimaal vijf (5) Beheerders kunnen tegelijkertijd actief werken in de Oplossing.

NF-E17	Business	Performance	Minimaal 50 Medewerkers, met een andere rol als Beheerder (bijvoorbeeld Content Ontwikkelaars of HR medewerkers) moeten tegelijkertijd kunnen werken in de backoffice omgeving van de Oplossing.
NF-E18	Business	Performance	Realtime rapportages mogen de performance van de Oplossing niet verminderen.
NF-E19	Business	Testbaarheid	De oplossing biedt tenminste een Productie-omgeving en een Test/Acceptatie-omgeving
NF-E20	Business	Testbaarheid	De Test/Acceptatie omgeving moet aangesloten kunnen worden op overeenkomstige testomgevingen van de gekoppelde SVB systemen.
NF-E21	Business	Schaalbaarheid	De Oplossing is schaalbaar. Als de beschikbare capaciteit tijdens Exploitatie onvoldoende blijkt dan wordt dit tijdig door Opdrachtnemer gesignaleerd en direct doorgegeven aan de SVB. De SVB kan er vervolgens voor kiezen om extra capaciteit af te nemen (tegen kosten en tarieven zoals vermeld in het Prijzenblad).
NF-E22	Business	Koppelingen	De Oplossing moet xAPI statements van diverse bronnen kunnen inlezen.
NF-E23	Business	Koppelingen	De Oplossing moet ook non-xAPI statements kunnen omzetten in xAPI. <i>Deze eis komt te vervallen</i>
NF-E24	Business	Koppelingen	De Oplossing moet data kunnen exporteren in alle gangbare formaten (waaronder .csv)
NF-E25	Business	Koppelingen	De Oplossing exporteert data in een formaat die kan worden ingelezen in tenminste Power BI.
NF-E26	Business	Koppelingen	De Oplossing moet data kunnen exporteren naar een externe database zoals een data warehouse.
NF-E27	Informatiebeheer	Metadata	Aan informatieobjecten moet metadata toegekend kunnen worden waaruit o.a. de inhoud, het proces, context en einddatum van een informatieobject duidelijk worden (bijv. een opleiding die niet meer gegeven wordt/vervangen is door een andere opleiding of een Medewerker die uit dienst is en waarvan de leerhistorie afgesloten is) zodat van de informatieobjecten duidelijk is waar het over gaat en hoe en wanneer het ontstaan is.
NF-E28	Informatiebeheer	Metadata	Informatieobjecten en bijbehorende metadata moeten in hun context (d.w.z. met behoud van onderlinge relaties tussen informatieobjecten, waaronder leerhistorie) geëxporteerd kunnen worden zodat het eventueel in een ander systeem gearchiveerd kan worden.
NF-E29	Informatiebeheer	Beheren van informatie	Bewaartermijnen moeten toegekend kunnen worden aan informatieobjecten die afgesloten zijn (archiveren) zodat deze informatieobjecten vernietigd kunnen worden ná het verstrijken van de bewaartermijn.
NF-E30	Informatiebeheer	Beheren van informatie	Rapportages (vernietigingslijsten) moeten gemaakt kunnen worden waaruit blijkt van welke informatieobjecten de bewaartermijn verlopen is zodat deze kunnen worden voorgelegd voor akkoord ter vernietiging.
NF-E31	Informatiebeheer	Beheren van informatie	Informatieobjecten moeten vernietigd kunnen worden zodat de SVB aan haar vernietigingsplicht vanuit de Archiefwet kan voldoen.
NF-E32	Informatiebeheer	Beheren van informatie	Vernietiging moet plaats kunnen vinden door een Medewerker Informatiebeheer ná akkoord van de proceseigenaar, hiervoor zijn rollen in het systeem beschikbaar zodat de te vernietigen informatieobjecten pas worden vernietigd ná het benodigde akkoord.

NF-E33	Informatiebeheer	Beheren van informatie	Een rapportage moet gemaakt en bewaard kunnen worden van vernietigde informatieobjecten (verklaring van vernietiging) zodat ook ná vernietiging inzichtelijk gemaakt kan worden welke informatieobjecten er zijn vernietigd.
NF-E34	Technische eisen	Koppelingen	De oplossing kan via het SMTP protocol worden aangesloten op op een e-mail gateway.
NF-E35	Technische eisen	Koppelingen	Koppelingen dienen minimaal beveiligd te zijn volgens de standaard TLS 1.2 of hoger.
NF-E36	Technische eisen	Koppelingen	Koppelingen zijn mogelijk via webservices en maken minimaal gebruik van SOAP/XML en REST/JSON.
NF-E37	Technische eisen	Koppelingen	De Oplossing biedt een directe mailfunctionaliteit via Microsoft 365 op basis van het SMTP protocol met ondersteuning van Modern Authentication. In de toekomst is moet aansluiting via Exchange Web Services met Modern Authentication mogelijk zijn.
NF-E38	Technische eisen	Koppelingen	Opdrachtnemer zorgt dat alle Koppelingen die in beheer zijn bij Opdrachtnemer (of diens toeleveranciers) blijven werken bij nieuwe releases en upgrades van de Oplossing. Deze Koppelingen vallen onder het informatiebeveiligingsbeleid van Opdrachtnemer en zijn onderdeel van de SLA.
NF-E39	Technische eisen	Koppelingen	Koppelingen die in beheer zijn bij Opdrachtnemer (of diens toeleveranciers) hebben duidelijke specificaties (descriptor documents).
NF-E40	Training	Documentatie	Opdrachtnemer levert voorafgaand aan de Transitie de noodzakelijke trainings-, en instructiematerialen van de Oplossing voor Beheerders, Ontwikkelaars en Back-office medewerkers, in de Nederlandse taal en in een voor de SVB aanpasbaar formaat, en houdt deze actueel gedurende de looptijd van de Overeenkomst.
NF-E41	Training	Ondersteuning	Opdrachtnemer verzorgt tijdens Transitie fase de noodzakelijke (online) trainingen en instructiesessies voor Beheerders, Ontwikkelaars en Back-office medewerkers om met de Oplossing te kunnen werken, en blijft minimaal een 4 weken na ingebruikname beschikbaar voor het beantwoorden van vragen achteraf (nazorg).
NF-E42	Financieel	Kortingen	Alle verleende kortingen van Aanbieders aan Opdrachtnemer voor Externe Leeractiviteiten die voor de SVB worden geboekt, komen ten goede aan de SVB.
NF-E43	Financieel	Facturatie	De SVB heeft het recht op inzage in de facturen die door Aanbieders aan Opdrachtnemer zijn verstuurd voor door Gebruikers gevolgde Externe Leeractiviteiten. Afschriften van deze facturen worden binnen 2 weken na schriftelijk verzoek van de SVB beschikbaar gemaakt.

Nummer	Hoofdcategorie	Subcategorie	Informatiebeveiliging & Privacy
IBP-E01	Informatiebeveiliging & Privacy	Eisen aan personeel	Alle medewerkers van de Opdrachtnemer die participeren in de levering van de Dienstverlening moeten aantoonbaar bekend zijn met de verantwoordelijkheid op het gebied van informatiebeveiliging en privacy die als onderdeel van zijn / haar rol van toepassing zijn.
IBP-E02	Informatiebeveiliging & Privacy	Eisen aan personeel	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de Dienstverlening een geheimhoudingsovereenkomst ondertekenen en hier naar handelen.
IBP-E03	Informatiebeveiliging & Privacy	Eisen aan personeel	Opdrachtnemer draagt zorg dat alle medewerkers die participeren in de levering van de Dienstverlening een specifiek voor de functie verstrekte Verklaring Omtrent Gedrag (VOG), of een gelijkwaardig document (in geval van een andere lidstaat), hebben die geldig is tijdens de duur van de uitvoering van de werkzaamheden.
IBP-E04	Informatiebeveiliging & Privacy	Algemeen	De Oplossing moet opgezet en geleverd worden vanuit het basis principe "Secure-by-Design".
IBP-E05	Informatiebeveiliging & Privacy	Algemeen	Opdrachtnemer heeft informatiebeveiliging en continuïteit aantoonbaar gestructureerd en gestandaardiseerd, en tevens een continue en procesmatige PDCA cyclus ingericht, op alle lagen van haar eigen organisatie (inclusief betrokken onderaannemers) en die van de Dienstverlening.
IBP-E06	Informatiebeveiliging & Privacy	Algemeen	De Dienstverlening en organisatie van de 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.
IBP-E07	Informatiebeveiliging & Privacy	Algemeen	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 Dienstverlening.
IBP-E08	Informatiebeveiliging & Privacy	Algemeen	Voor het uitvoeren van onderhoud en/of aanpassingen van de Dienstverlening 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.
IBP-E09	Informatiebeveiliging & Privacy	Algemeen	Opdrachtnemer dient zorg te dragen dat software welke gebruikt wordt als onderdeel van de Oplossing, altijd wordt ondersteund door de leverancier van de software en blijft functioneren binnen de SVB werkomgeving.
IBP-E10	Informatiebeveiliging & Privacy	Clouddiensten	Verwerking van (waaronder toegang tot) data van de SVB moet uitsluitend plaatsvinden binnen de Europese Economische Ruimte (Europese Unie, Noorwegen, Liechtenstein, IJsland).
IBP-E11	Informatiebeveiliging & Privacy	Clouddiensten	Alle Koppelingen tussen de Oplossing en bron-en doelsystemen van de SVB moeten op basis van open standaarden 'comply or explain' plaatsvinden.
IBP-E12	Informatiebeveiliging & Privacy	Clouddiensten	SVB-gegevens zijn altijd logisch en functioneel gescheiden van die van de overige afnemers c.q. klanten van Opdrachtnemer.

IBP-E13	Informatiebeveiliging & Privacy	Clouddiensten	In het kader van dataportabiliteit moet Opdrachtnemer de volgende voorzieningen binnen de contractueel gedefinieerde termijn ter beschikking stellen voor het exporteren van data (na beëindiging van de dienstverlening): Data moet beschikbaar zijn in een voor de SVB bruikbaar format zoals CSV, Excel (xlsx) en PDF (1.7). In het geval er sprake is van aanlevering van documenten tijdens gebruik van de dienst, dan moet het “originele / oorspronkelijke” format van het document (inclusief mappenstructuren) beschikbaar zijn.
IBP-E14	Informatiebeveiliging & Privacy	Risico analyses	Opdrachtnemer heeft procedures om analyseren van risico's te borgen in het kader van de Dienstverlening. De (opvolging van de) voor de SVB relevante (IB)-risico's en mitigerende maatregelen worden besproken en waar nodig belegd, opgevolgd en meegenomen in de met de SVB afgesproken rapportagecyclus.
IBP-E15	Informatiebeveiliging & Privacy	Risico analyses	Opdrachtnemer legt bekende risico's vast in een register en deze wordt door Opdrachtnemer voorzien van de nodige (borgings-)maatregelen ter mitigatie van de risico's.
IBP-E16	Informatiebeveiliging & Privacy	Risico analyses	Opdrachtnemer moet de SVB direct op de hoogte stellen van risico's die de classificatie “hoog” bestempeld krijgen, zoals vastgelegd in het risicoregister (zie IBP-E15).
IBP-E17	Informatiebeveiliging & Privacy	Risico analyses	Minimaal eens per kwartaal moet er worden gerapporteerd over de status van de risico's en de bijbehorende (voortgang van de) mitigerende maatregelen.
IBP-E18	Informatiebeveiliging & Privacy	Logische toegangsbeveiliging	Opdrachtnemer stelt de SVB in staat om aan te tonen dat er betrouwbare, effectieve en controleerbare mechanismen worden ingezet voor het vastleggen en vaststellen van de identiteit van gebruikers, en het toekennen van rechten aan gebruikers bij het gebruik van de Dienstverlening) door gebruikers. Onder gebruikers (met een kleine letter 'g') worden hier, en in de overige IBP eisen, verstaan alle Medewerkers die op enige wijze gebruik maken van de Dienstverlening of toegang hebben tot de Oplossing.
IBP-E19	Informatiebeveiliging & Privacy	Logische toegangsbeveiliging	De Dienstverlening moet afdwingen dat gebruikers alleen toegang hebben tot informatie, beheertaken en speciale bevoegdheden voor zover dat voor de uitoefening van de werkzaamheden noodzakelijk is (“need to know”, “need to use”, “least privilege”) en ze hiervoor herleidbaar geautoriseerd zijn.
IBP-E20	Informatiebeveiliging & Privacy	Logische toegangsbeveiliging	De Oplossing moet kunnen koppelen aan de IDaaS (Identity as a Service) waarbij de koppeling op basis van open standaarden moet worden vormgegeven.
IBP-E21	Informatiebeveiliging & Privacy	Logische toegangsbeveiliging	Voor applicaties die onderdeel zijn van de Oplossing en vereisen dat een set van identiteitsinformatie van gebruikers in het systeem aanwezig is, moet gebruik worden gemaakt van automatische provisioning. De SVB is hierbij verantwoordelijk voor het vaststellen van de filtering van de accountattributen die geprovisioned worden.
IBP-E22	Informatiebeveiliging & Privacy	Logische toegangsbeveiliging	Opdrachtnemer is verantwoordelijk voor het periodiek (minimaal eens per kwartaal) controleren van de toegangsrechten van Medewerkers die werkzaamheden uitvoeren ten behoeve van de Dienstverlening.

IBP-E23	Informatiebeveiliging & Privacy	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.
IBP-E24	Informatiebeveiliging & Privacy	Vulnerability management	Opdrachtnemer moet borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd en zorgt dat installatie van nieuwe patches geen afbreuk doet aan de continuïteit en beschikbaarheid van de Dienstverlening.
IBP-E25	Informatiebeveiliging & Privacy	Vulnerability management	Voor ingebruikname van een nieuwe dienst / ICT component en bij een significante wijziging van de Oplossing moet een kwetsbaarheidscans uitgevoerd worden en moeten de bevindingen opgelost worden.
IBP-E26	Informatiebeveiliging & Privacy	Vulnerability management	Opdrachtnemer rapporteert periodiek (minimaal eens per kwartaal) over de resultaten van de kwetsbaarheidscans en de daarbij behorende (voorgestelde) mitigerende maatregelen.
IBP-E27	Informatiebeveiliging & Privacy	Patch management	Patch management moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de Dienstverlening en borgen dat de meest recente (beveiligings)patches zijn geïnstalleerd.
IBP-E28	Informatiebeveiliging & Privacy	Patch management	Indien een (beveiligings)patch beschikbaar is, moeten de risico's verbonden aan de installatie van de patch worden geëvalueerd en moet de patch getest worden alvorens deze op productiesystemen wordt toegepast.
IBP-E29	Informatiebeveiliging & Privacy	Patch management	Opdrachtnemer rapporteert periodiek (minimaal eens per kwartaal) over de resultaten van het patch management proces en de daarbij behorende (eventuele) afwijkingen en/of risico's.
IBP-E30	Informatiebeveiliging & Privacy	Security Hardening	Security hardening moet procesmatig, ondersteund door gestandaardiseerde en vastgestelde richtlijnen, worden uitgevoerd op alle ICT-systemen van de Oplossing.
IBP-E31	Informatiebeveiliging & Privacy	Security Hardening	Bij het vaststellen en toepassen van de security hardening richtlijnen moet minimaal onderscheid gemaakt worden tussen de volgende ICT componenten: - Applicaties; - Middleware en databases; - Platformen / infrastructuur; - Netwerken; - Connectiviteit.
IBP-E32	Informatiebeveiliging & Privacy	Security Hardening	Opdrachtnemer hanteert internationaal erkende security hardening standaarden, (de CIS (Center of Internet Security) benchmarks), als basis voor het vaststellen van de security hardening richtlijn voor de ICT componenten.
IBP-E33	Informatiebeveiliging & Privacy	Security Hardening	Opdrachtnemer toetst periodiek (minimaal eens per kwartaal) alle ICT componenten op basis van de vastgestelde richtlijn en rapporteert de resultaten als onderdeel van de kwartaalrapportage. Geconstateerde afwijkingen worden hierin, na analyse, op basis van risico inschatting benoemd.

IBP-E34	Informatiebeveiliging & Privacy	Penetratietesten	De SVB heeft het recht om een pentest uit te laten voeren om de beveiliging te testen in het kader van de 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.
IBP-E35	Informatiebeveiliging & Privacy	Penetratietesten	Penetratietesten moeten procesmatig en procedureel, ondersteund door richtlijnen, worden uitgevoerd op alle ICT componenten van de Oplossing.
IBP-E36	Informatiebeveiliging & Privacy	Penetratietesten	Opdrachtnemer heeft een procedure om bij significante wijzigingen (bijvoorbeeld in gebruikname nieuwe dienst/ICT componenten) in het kader van de 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.
IBP-E37	Informatiebeveiliging & Privacy	Penetratietesten	Opdrachtnemer rapporteert in het kader van de Dienstverlening de resultaten van de penetratietesten direct aan de SVB en legt vervolgens periodiek (minimaal eens per kwartaal) verantwoording af over de opvolging van de bevindingen.
IBP-E38	Informatiebeveiliging & Privacy	Webapplicatie	Opdrachtnemer dient bij het ontwikkelen, implementeren en beheren van de Dienstverlening de principes "Security by Design" (secure software development) en "Privacy by Design and Default" toe te passen.
IBP-E39	Informatiebeveiliging & Privacy	Webapplicatie	Opdrachtnemer beschikt over passende en aantoonbare maatregelen en beleid zodat de Dienstverlening voldoet aan de NCSC ICT-Beveiligingsrichtlijnen voor Webapplicaties. https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties
IBP-E40	Informatiebeveiliging & Privacy	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 Dienstverlening.
IBP-E41	Informatiebeveiliging & Privacy	Webapplicatie	In het kader van opslag en/of transport van persoonsgegevens moet de Oplossing voldoen aan de cryptografische beveiligingsvoorzieningen zoals voorgeschreven in de NCSC ICT-Beveiligingsrichtlijnen voor Transport Layer Security (TLS). https://www.ncsc.nl/onderwerpen/verbodingsbeveiliging/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1
IBP-E42	Informatiebeveiliging & Privacy	Infrastructurele beveiligingseisen	Als onderdeel van de architectuur van de Oplossing moet netwerksegmentatie / zonering conform een "defense in depth" strategie worden toegepast.
IBP-E43	Informatiebeveiliging & Privacy	Infrastructurele beveiligingseisen	De Dienstverlening (incl. te gebruiken componenten) 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.

IBP-E44	Informatiebeveiliging & Privacy	Infrastructurele beveiligingseisen	De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT systemen moeten regelmatig worden gemonitord (bewaakt, geanalyseerd) en de bevindingen periodiek gerapporteerd als onderdeel van het informatiebeveiliging incidentenproces.
IBP-E45	Informatiebeveiliging & Privacy	Infrastructurele beveiligingseisen	De Dienstverlening moet alleen toegankelijk zijn via door de SVB goedgekeurde endpoints en op de SVB goedgekeurde wijze.
IBP-E46	Informatiebeveiliging & Privacy	Privacy	De Dienstverlening moet gedurende de gehele looptijd van de Overeenkomst voldoen aan de algemene vigerende wet- en regelgeving van de Nederlandse overheid, waaronder de AVG (Algemene Verordening Gegevensbescherming).
IBP-E47	Informatiebeveiliging & Privacy	Privacy	In lijn met Verwerkersovereenkomst moet de Opdrachtnemer 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 overeengekomen, en zal de Opdrachtnemer de persoonsgegevens dus niet gebruiken voor het uitvoeren van testen en/of het uitvoeren van data-analyses.
IBP-E48	Informatiebeveiliging & Privacy	Privacy	Daar waar de SVB geen volledige toegang heeft tot de persoonsgegevens moet Opdrachtnemer de SVB ondersteunen bij verzoeken tot inzage, correctie en eventueel het wissen van persoonsgegevens.
IBP-E49	Informatiebeveiliging & Privacy	Privacy	De Dienstverlening moet de mogelijkheid bieden om gegevenscomponenten die niet strikt noodzakelijk zijn voor latere verwerkingen of waarvoor geen doelbinding of rechtsgrond aanwezig is, te verwijderen of te verbergen.
IBP-E50	Informatiebeveiliging & Privacy	Clouddiensten	De Oplossing versleutelt alle gegevens in de cloud waarbij gebruik gemaakt wordt van de geldende 'best practices' (afhankelijk van de stand der techniek) m.b.t. versleuteling.
IBP-E51	Informatiebeveiliging & Privacy	Clouddiensten	De bij Opdrachtnemer gebruikte encryptiesleutels voor het encrypten van de data binnen de Oplossing moet op elk moment in het proces per direct ingetrokken of onbruikbaar kunnen worden gemaakt.
IBP-E52	Informatiebeveiliging & Privacy	Clouddiensten	Bij multi-tenancy worden alle gegevens die binnen de Oplossing worden opgeslagen of verwerkt ten behoeve van de SVB versleuteld en gescheiden verwerkt op gehardende (virtuele) machines.

IBP-E53	Informatiebeveiliging & Privacy	Privacy	Bij toepassing van data-protection-by default door Opdrachtnemer moeten tenminste de volgende aspecten meegewogen worden: 1. Gedurende het systeemontwikkelp proces moet continue rekening gehouden worden met de privacy van gebruikers. De belangen en privacy van betrokkene dienen centraal te staan. Bijvoorbeeld er is geen opt-out regime, maar opt-in: pas als iemand zich ergens voor heeft aangemeld ontvangt hij informatie (opt-in), niet het automatisch ontvangen totdat het wordt stopgezet (opt-out). 2. Bij het inrichten van autorisatie rollen moet rekening gehouden worden met privacy en worden alleen die persoonsgegevens getoond die een medewerker nodig heeft voor zijn functie. 3. Beperk zoekfunctionaliteit m.b.t. persoonsgegevens en geef alleen zoekresultaten weer na het invoeren van een aantal persoonsgegevens. 4. Pas whitelisting toe voor het opvragen van persoonsgegevens. De sterkte van whitelisting is afhankelijk van de implementatie van de whitelist. Een goede toepassing is dat de whitelist wordt samengesteld door een mechanisme/tooling die onafhankelijk is van de gebruiker (bv. een workflow-systeem waarmee de gebruiker alleen toegang krijgt tot persoonsgegevens van de betrokkene waar hij op dat moment mee bezig is).
IBP-E54	Informatiebeveiliging & Privacy	Privacy	Voor de Dienstverlening moet, waar relevant, verwijderen en bewaren zijn ingericht m.b.t. persoonsgegevens met voldoende (meta)data om de context van de betreffende data te kunnen herleiden.
IBP-E55	Informatiebeveiliging & Privacy	Privacy	Voor de Dienstverlening moet verwijderen (oa ihkv bewaartermijnen) zijn ingericht met betrekking tot tijdelijke bestanden en/of logs waarin persoonsgegevens staan. De tijdelijke bestanden en/of logs wordt in ieder geval niet langer bewaard dan maximaal 13 maanden.
IBP-E56	Informatiebeveiliging & Privacy	Privacy	Tijdelijke bestanden e/o logs met betrekking tot de Dienstverlening moeten 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.
IBP-E57	Informatiebeveiliging & Privacy	Beveiligingsincidenten	Opdrachtnemer meldt informatiebeveiligingsincidenten, waaronder maar niet beperkt tot datalekken, direct en in ieder geval binnen 24 uur per e-mail bij de SVB Servicedesk, op het emailadres: servicedesk@svb.nl.
IBP-E58	Informatiebeveiliging & Privacy	Beveiligingsincidenten	In het geval van een informatiebeveiligingsincident moet Opdrachtnemer direct maatregelen treffen om de gevolgen en de schade te beperken voortkomend uit het incident.
IBP-E59	Informatiebeveiliging & Privacy	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 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.

IBP-E60	Informatiebeveiliging & Privacy	Controle en 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 ihkv de Dienstverlening en deze dienen meegenomen te worden bij de doorontwikkeling van de Oplossing en zo nodig op de kortst mogelijke termijn te worden gepatcht.
IBP-E61	Informatiebeveiliging & Privacy	Controle en Audits	Opdrachtnemer draagt in het kader van de Dienstverlening jaarlijks zorg voor inzicht (in overleg e/o in rapportage) in onderstaande onderwerpen: - De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; - Overzicht van afwijkingen ten opzichte van beleid of contract; - Overzicht van de risico acceptatie; en - Een recente onafhankelijke audit-verklaring die past bij de aard van de Dienstverlening (zoals een ISAE 3000 rapportage op basis van één of meerdere SOC2 – Trusted Services Principles, of gelijkwaardig).
IBP-E62	Informatiebeveiliging & Privacy	Overleg & rapportage	Opdrachtnemer stelt een vaste contactpersoon aan die voor de Dienstverlening verantwoordelijk is voor zowel informatiebeveiliging als privacy.
IBP-E63	Informatiebeveiliging & Privacy	Overleg & rapportage	Gestructureerd en periodiek (minimaal eens per kwartaal) dient overleg tussen Opdrachtnemer en SVB plaats te vinden om zowel de rapportages als (eventuele) issues te bespreken.
IBP-E64	Informatiebeveiliging & Privacy	Overleg & rapportage	Opdrachtnemer moet zorgen voor een rapportage waarmee verantwoording wordt afgelegd over de mate van invulling en effectiviteit van de getroffen beveiligingsmaatregelen en het gerealiseerde beveiligingsniveau (inclusief privacy) binnen de scope van de Dienstverlening.
IBP-E65	Informatiebeveiliging & Privacy	Overleg & rapportage	Elk kwartaal moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de Dienstverlening): - Een overzicht van de beveiligingsincidenten (inclusief datalekken) inclusief trends, evaluaties en (root cause) analyses; - Rapportages van risico's, kwetsbaarheden (vulnerability scan resultaten), patch management, hardening afwijkingen en voortgangsrapportages over bijbehorende remediation plannen; en - Analyse van de logging en monitoring informatie.
IBP-E66	Informatiebeveiliging & Privacy	Overleg & rapportage	Jaarlijks moeten onderstaande rapportage-vereisten worden ingevuld (specifiek voor de Dienstverlening): - De status, handhaving en effectiviteit van de geïmplementeerde maatregelen; - Overzicht van afwijkingen ten opzichte van beleid of contract; en - Overzicht van de risico acceptatie.
IBP-E67	Informatiebeveiliging & Privacy	Tracking en tracing / logging	Alle activiteiten moeten gelogd worden in een logbestand.
IBP-E68	Informatiebeveiliging & Privacy	Infrastructurele beveiligingseisen	Malicieuze activiteiten worden gesignaleerd op basis van door SVB te bepalen regels en gelogd in het logbestand.

IBP-E69	Informatiebeveiliging & Privacy	Tracking en tracing / logging	De logbestanden kunnen niet achteraf worden aangepast.
IBP-E70	Informatiebeveiliging & Privacy	Tracking en tracing / logging	Opdrachtnemer dient de logbestanden met betrekking tot het gedrag van de gebruikers en de toegang en handeling door medewerkers van Opdrachtnemer op de SVB-data, binnen de Oplossing beschikbaar te stellen aan de SVB. Dit middels een nader overeen te komen timing, gangbaar format en overdracht-mechanisme tussen de SVB en de Opdrachtnemer waarbij een adequate bescherming van deze data wordt toegepast.
IBP-E71	Informatiebeveiliging & Privacy	Tracking en tracing / logging	Het is configureerbaar welke informatie van transacties in de logbestanden wordt bewaard.
IBP-E72	Informatiebeveiliging & Privacy	Beveiligingsincidenten	Opdrachtnemer heeft monitoring-, meld- en responsprocedures geïmplementeerd (en evalueert periodiek de effectiviteit daarvan) om informatiebeveiligingsincidenten (waaronder datalekken m.b.t. persoonsgegevens) te detecteren, melden en de gevolgen daarvan te mitigeren.
IBP-E73	Informatiebeveiliging & Privacy	Infrastructurele beveiligingseisen	De SVB hanteert een defense-in-depth strategie. Opdrachtnemer dient de SVB in staat te stellen onderbouwd aan te kunnen tonen dat de Oplossing voldoet aan deze strategie.

Nummer	Hoofdcategorie	Subcategorie	Service Level Requirements
SLR-E1	Servicemanagement	SLA	De definitieve Service Level Agreement zal voorafgaand aan ondertekening van de Overeenkomst, door Opdrachtnemer worden opgesteld in overeenstemming met de hieronder gestelde Eisen en door Opdrachtnemer ingevulde wensen, en ter goedkeuring aan de SVB worden voorgelegd.
SLR-E2	Servicemanagement	Helpdesk	De Opdrachtnemer stelt een Nederlandstalige Helpdesk beschikbaar die tweedelijns ondersteuning levert aan Beheerders, Ontwikkelaars en Backoffice medewerkers..
SLR-E3	Servicemanagement	Helpdesk	De Helpdesk stelt zich klantvriendelijk op en afspraken worden in heldere bewoordingen geregistreerd.
SLR-E4	Servicemanagement	Beschikbaarheid	De Beschikbaarheid van de Dienstverlening is minimaal 98% op maandbasis
SLR-E5	Servicemanagement	Beschikbaarheid	Alle schermwisselingen moet binnen 2 seconden getoond worden
SLR-E6	Servicemanagement	Beschikbaarheid	De Helpdesk heeft alle Incidenten binnen de volgende richtlijnen opgelost: Prio 1: 95% < 4 uur Prio 2: 95% < 8 uur Prio 3: 95% < 16 uur Prio 4: 95% < 50 uur Prio 5: 95% < 120 uur
SLR-E7	Servicemanagement	Beschikbaarheid	Geplande onderhoudswerkzaamheden waardoor Gebruikers, Beheerders of Ontwikkelaars niet meer ongestoord gebruik kunnen maken van de Dienstverlening, worden door Opdrachtnemer niet uitgevoerd op werkdagen tussen 08:00 en 17:00.
SLR-E8	Servicemanagement	Beschikbaarheid	Opdrachtnemer zorgt voor back-ups (en restoremogelijkheden) zodat er maximaal 24 uur dataverlies kan optreden. Opdrachtnemer is verantwoordelijk voor controle van de integriteit van die back-ups, alsmede het waarborgen van de vertrouwelijkheid en beschikbaarheid daarvan.
SLR-E9	Servicemanagement	Beschikbaarheid	Opdrachtnemer zorgt ervoor dat Incidenten op de Productie-omgeving binnen 5 minuten worden gedetecteerd en Beheerders en Ontwikkelaars hiervan schriftelijk op de hoogte worden gesteld.
SLR-E10	Servicemanagement	Beschikbaarheid	Opdrachtnemer zorgt ervoor dat Incidenten op de productie-omgeving binnen 5 minuten worden gedetecteerd en Gebruikers desgewenst een melding te zien krijgen in het LeerEcoSysteem.
SLR-E11	Servicemanagement	Beschikbaarheid	Opdrachtnemer moet bij een calamiteit of uitwijktest in staat zijn om binnen een werkdag de koppelvlakken aan te passen naar de nieuwe locatie.
SLR-E12	Servicemanagement	Tracking en tracing / logging	Opdrachtnemer heeft beheerprocessen ingericht en hanteert een managementsysteem om Incidenten te registreren en te volgen. In geval van een Incident krijgt de SVB een notificatie uit dit systeem per email bij registratie, voortgang en oplossing.
SLR-E13	Servicemanagement	Tracking en tracing / logging	Beheerders kunnen bepalen voor welke Incidenten een mailnotificatie uit het managementsysteem wordt verstuurd en naar welke doelgroepen.
SLR-E14	Servicemanagement	Tracking en tracing / logging	Registratie van een Incident bevat minimale informatie (zoals aanleiding, tijdstip, aard en context van de opgetreden storing) voor Beheerders om zo mogelijk zelf storingen te kunnen herstellen.

SLR-E15	Servicemanagement	Overleg & rapportage	Opdrachtnemer geeft maandelijks inzicht in de geleverde prestaties, middels een SLA rapportage op de afgesproken Service Levels. Deze SLA rapportages zijn goed leesbaar, duidelijk en volledig.
SLR-E16	Servicemanagement	Overleg & rapportage	Opdrachtnemer rapporteert (indien van toepassing) regelmatig over de voortgang van de realisatie van alle eventuele verbeterplannen naar aanleiding van voorgekomen Incidenten.
SLR-E17	Servicemanagement	Overleg & rapportage	Opdrachtnemer heeft een vastomlijnde aanpak en/of managementsysteem voor de borging en continue verbetering van de kwaliteit van haar dienstverlening.
SLR-E18	Servicemanagement	Overleg & rapportage	Opdrachtnemer biedt een Single Point Of Contact voor escalatie door de SVB in het geval van zwaarwegende problemen met communicatie, incidenten of andere zaken.
SLR-E19	Servicemanagement	Overleg & rapportage	Indien sprake is van een tekortschietende Dienstverlening treden partijen met elkaar in overleg om herhaling te voorkomen en nakoming van de Overeenkomst zeker te stellen, waarbij meerdere escalatieniveaus zijn te doorlopen. De SVB zal voorafgaand aan dat overleg schriftelijk aan de Opdrachtnemer aangeven op welke punten de Dienstverlening is tekortgeschoten.
SLR-E20	Servicemanagement	Overleg & rapportage	Opdrachtnemer signaleert gevraagd en ongevraagd potentiële problemen die ook buiten de scope en reikwijdte van de Overeenkomst vallen, en komt met relevante verbetervoorstellen.
SLR-E21	Servicemanagement	Overleg & rapportage	De communicatie tussen de SVB en Opdrachtnemer in brede zin verloopt op een professionele en toegankelijke wijze.
SLR-E22	Servicemanagement	Brokerdienstverlening	Na een verzoek van de SVB voor Maatwerk levert de Broker binnen drie (3) weken drie (3) passende offertes aan de SVB.
SLR-E23	Servicemanagement	Brokerdienstverlening	Na de keuze door SVB voor een Maatwerk offerte, komt de Leeractiviteit binnen 10 dagen beschikbaar in het LeerEcoSysteem.
SLR-E24	Servicemanagement	Divers	Opdrachtnemer denkt mee met de SVB in het beheersen van de dagelijkse problematiek, werkt goed samen met de SVB en stelt zich op als een partner van de SVB.
SLR-E25	Servicemanagement	Divers	Opdrachtnemer fungeert als schakel tussen materie en techniek, bezit hiervoor voldoende IT-kennis en materiedeskundigheid, en is in staat om op een strategisch niveau met de SVB mee te denken.
SLR-E26	Servicemanagement	Divers	Opdrachtnemer denkt mee over de consequenties van door de SVB gedane wijzigingsvoorstellen, en wijst op de mogelijke gevolgen als deze wijzigingsvoorstellen een negatieve impact kunnen hebben.