



**Inkoop Uitvoering Centrum**

**Bezoekadres**

Prinses Beatrixlaan 2  
2595 AL Den Haag

**Postadres**

Postbus 93144  
2509 AC Den Haag

[www.rvo.nl](http://www.rvo.nl)

**Behandeld door**

Anouk Schatorje

**Ons kenmerk**

202101084

**Datum**

24 juni 2021

# verslag

Verslag marktconsultatie in verband met optimale LIMS ondersteuning van het laboratorium NRC

## Inleiding

Ter voorbereiding op een eventuele aanbesteding die voorziet in de ondersteuning van de informatievoorziening binnen het Nationaal Referentie Centrum (NRC), heeft de Nederlandse Voedsel- en Warenautoriteit (NVWA) op 23 april 2021 een marktconsultatie gepubliceerd op TenderNed.

## Beoogd doel

De marktconsultatie moet inzicht verschaffen over de mogelijkheden die er zijn om de behoefte in te vullen. En met name:

- of er voldoende interesse en capaciteit is in de markt voor de opdracht;
- het toetsen van eigen beeld aan de markt;
- of er innovatieve oplossingen zijn, dan wel alternatieve oplossingsrichtingen.

## Procedure

Op 25 mei 2021 zijn in een nota van inlichtingen vragen beantwoord die door geïnteresseerde leveranciers gesteld waren naar aanleiding van de gepubliceerde aankondiging.

Aan de markt is gevraagd 41 vragen te beantwoorden. In totaal hebben zeven leveranciers gereageerd. Bij vijf leveranciers had de NVWA behoefte aan een nadere toelichting. Dit is verstrekt door middel van een 1 op 1 gesprek op 10 juni 2021. In dit document vindt u per vraag de verschillende antwoorden op hoofdlijnen. Bij de mogelijke aanbesteding zal dit verslag openbaar gepubliceerd worden.

De NVWA wil de deelnemende leveranciers danken voor de gegeven input op de vragen in het marktconsultatiedocument. Neem gerust contact op wanneer u vragen heeft over dit verslag van de marktconsultatie. U kunt de betrokken inkoopadviseur (Anouk Schatorje) bereiken via TenderNed.

Hieronder de vragen en bijbehorende antwoorden van de leveranciers. Indien mogelijk begint elk antwoord met een korte samenvatting. Door de diversiteit zijn de antwoorden niet altijd samen te vatten. Vervolgens worden de antwoorden opgesomd. De onderdelen van de samenvatting worden hierin niet herhaald.

### 1.1 LIMS specifieke functionaliteiten

De NVWA heeft de leveranciers gevraagd om bij een aantal vragen aan te geven op welke manier hun oplossing de gewenste functionaliteit kan bieden. Zie hieronder de mogelijkheden:

1. Out of the box: functionaliteit is direct beschikbaar in de oplossing.
2. Configureerbaar: functionaliteit is in de oplossing in te stellen, zonder te programmeren.
3. Maatwerk: functionaliteit moet worden geprogrammeerd.

Per vraag wordt in de hieronder afgebeelde tabel aangegeven hoeveel leveranciers het op de betreffende manier kunnen aanbieden.

|                |  |
|----------------|--|
| Configuurbaar  |  |
| Out of the box |  |
| Maatwerk       |  |

De oplossingen verschillen in out of box functionaliteit, configureerbaarheid of de mate van maatwerk. Door de verschillende leveranciers worden zowel pakketten als platforms aangeboden.

1. *Op dit moment dienen de onderzoekers in het laboratorium gebruik te maken van papieren formulieren voor het invullen van beoordelingen tijdens de analyses. Vervolgens worden deze beoordelingen op een later moment in het huidige LIMS geplaatst. In de toekomst willen we zoveel mogelijk papierloos werken en digitaliseren. Welke digitale middelen kunt u aanbieden gericht op de laboratorium context binnen het NRC (neem hierin in ieder geval mee het werken met technieken ELISA: Enzyme Linked Immuno Sorbent Assay en PCR: Polymerase chain reaction)?*

|                |   |
|----------------|---|
| Configuurbaar  | 4 |
| Out of the box | 3 |
| Maatwerk       | 2 |

Samenvatting:

De leveranciers ondersteunen papierloos werken op meerdere en verschillende manieren. De analysetechnieken ELISA en PCR worden niet door elke leverancier genoemd in de beantwoording.

Beantwoording:

- Koppelingen met laboratoriuminstrumenten en het LIMS, meetresultaten geautomatiseerd ingelezen in het LIMS. Onder andere de volgende communicatiestandaarden worden ondersteund: HL7, XML, CSV, etc.
- Optimaliseren van rechtstreekse invoer in LIMS, door middel van plausibiliteitscontroles, invulsjablonen en vrije tekst. Meerdere leveranciers geven aan gebruik te maken van plausibiliteitscontroles.
- Werken met spraakherkenning, invoer van korte vaste stukjes informatie (al dan niet gecodeerd) worden versneld door gebruik te maken van barcodes en barcodescanning.
- Papieren documenten kunnen ten alle tijde worden gescand en als digitaal document aan een dossier worden toegevoegd (indien nodig).
- Elektronisch Laboratorium Notebook (ELN) die is ontworpen om wetenschappers het ultieme platform te bieden om zowel gestructureerde als ongestructureerde data vast te leggen tijdens laboratorium werkzaamheden. Een andere partij geeft aan met de beschikbare document management functionaliteit kan ook de volledige implementatie/projectdocumentatie volledig digitaal worden vastgelegd en beheerd in het systeem.
- Volledig functionele module voor Plate handling t.b.v. o.a. ELISA en PCR, ook genoemd door een andere leverancier visualisering Microplates (ondersteuning van ELISA en PCR).
- Geautomatiseerd robot aansturen en importeren van resultaten. Vastleggen van uw Plate protocollen, filling, QC's en opslag van uw plates met volledig ondersteund locatie beheer. Plate protocol omvat o.a. Plate layout, filling instructions, connectie Liquid Handling Robot, Identification, etc.
- Een flexibele voorraadbeheermodule die kan worden gebruikt om voorraadinformatie van opgeslagen monsters, chemicaliën e/o materialen te beheren, inclusief de hoeveelheden reserves die tijdens de levensduur van het onderzoek zijn opgeslagen en gebruikt. Monsters kunnen indien nodig tussen locaties worden verplaatst, met volledige audittrail en traceerbaarheid.
- Inventory Manager maakt het mogelijk om elk type materiaal , op te slaan en bij te houden. Voorraad kan worden aangepast en verplaatst, hoeveelheden kunnen bijgehouden worden, waar het is en wie er verantwoordelijk voor is. Het is mogelijk om voorraadartikelen samen te voegen. Regels voor het automatisch verlagen van voorraadniveaus kunnen worden ingesteld met betrekking tot laboratoriumbewerkingen en workflows.
- Sample- of Order-Intake, planning en controle van samples, workflow/distributie van samples.
- Registratie van gemeten waarden, grenswaardebewaking en resultaat validatie.

- Voorbereiding, verspreiding en archivering van rapportage, certificaten, statistieken en evaluaties.
- Digitale signature, Capaciteitsplanning, Material Management van Chemicaliën en Reagentia.
- WebPortal t.b.v. beschikbaar stellen sample/order informatie in Portal omgeving.
- Mobile Data functionaliteit t.b.v. digitaliseren werkzaamheden buiten de labomgeving.
- CRM functionaliteit voor Offertes en facturatie van laboratoriumdiensten
- Automatiseringsplatform gebaseerd op de nieuwste technologieën (o.a. Cloud, Web, en Mobile technology).
- Mobiele responsieve Web technologie, volledig digitaal te werken door onderzoeksprocessen te stroomlijnen en routinehandelingen te automatiseren – ook in streng gereguleerde omgevingen.
- Configureerbare Entiteiten-model, sjablonen die dienen om de vereiste functionaliteiten en processtromen te configureren. Nieuwe kenmerken/attributen kunnen aan entiteiten worden toegevoegd en geconfigureerd. De beschikbare entiteiten bieden de NVWA alle benodigde functionaliteit om de uitlopende analysetechnieken (ELISA, PCR, ...) efficiënt te automatiseren. Volledig digitale overdracht van data tussen de centrale database en benodigde laboratorium instrumenten/apparaten te bewerkstellingen en bestaande ondersteunende randapparatuur te koppelen (bijv. scanners) en geautomatiseerd aan te sturen (bijv. printopdrachten).
- ProcessStations & Visuele workflow, waar traditionele systemen workflows veelal benaderen als één geheel en deze in één keer dienen te worden uitgevoerd, biedt de oplossing de mogelijkheid om alle type routinematige processen bestaande uit 1 of meerdere stappen efficiënt en volledig digitaal uit te voeren. Eindgebruikers worden in Process Stations begeleid in de stappen die er gedaan moeten doen. De oplossing gaat verder dan eenvoudige werklijsten aangezien alle processtappen in een Process Station kunnen worden geregistreerd en daarmee automatisch gedigitaliseerd voor rapportage! Door de zelf-documenterende werking neemt de documentatie effort met forse schreden af. Met de Process Stations wordt de mogelijkheid geboden om de benodigde flexibiliteit per laboratorium/afdeling en per analyse/bepaling specifieke processen efficiënt en naar wens in te richten. Aan de hand van deze Process Stations kunnen gebruikers intuïtief en stap voor stap door een process worden geleid waarbij per stap enkel de informatie/actie/instructie wordt getoond die nodig is om de stap uit te voeren. Daarbij kunnen Process Station stappen automatisch middels barcode-scan acties worden aangestuurd.
- Met behulp van zogenaamde dynamische Image Maps kunnen werkstromen goed inzichtelijk worden gemaakt en gebruikt worden als intuïtieve leidraad door een analyseproces voor eindgebruikers.
- Planning & Scheduling functionaliteit biedt de mogelijkheid de werkvoorraad in kaart te brengen en (automatisch) optimale planningen te genereren voor de uitvoering. Deze planning en voortgang kan voor elke afdeling apart in kaart worden gebracht. De planning kan volledig digitaal "gedeeld" worden met alle betrokkenen zowel intern als extern

aan de organisatie door middel van overzichten, real-time dashboards en rapportages.

- Door de web based oplossing kan data eenvoudig en real-time worden gedeeld en getoetst door interne en externe gebruikersgroepen en/of opdrachtgevers. De beschikbare Portal functionaliteit kan de samenwerking met diverse int en externe opdrachtgevers en ander belanghebbenden enorm vergemakkelijken. Ook biedt het platform de mogelijkheden zaken digitaal af te tekenen, te rapporteren en volledig onder versie & audit beheer te laten vallen.
- Support several type of results, including text result (in html format, close to a word).
- Wij kunnen met PCR apparatuur koppelen. Wij geven de voorkeur aan gebruik van standaarden, dit is zo stabiel mogelijk. Gebruikelijk is bijvoorbeeld XML koppelingen. In de praktijk zijn soms ook alternatieve oplossingen nodig.

2. *Na binnenkomst van het monster bij het NRC wordt het monster gecontroleerd en vervolgens toegekend aan een vakgebied, die het monster in behandeling neemt. Dit vakgebied voert verschillende analyses uit, stelt een diagnose op en verstuurd de terugkoppeling. Als onderdeel van het analyse proces kan het vakgebied een taak uitzetten bij een ander vakgebied. Gedurende dit proces worden in verschillende vormen informatie en foto's vastgelegd over het monster, die op een later moment snel terug te vinden moeten zijn.*

*Kunt u schetsen op welke wijze de dossiervorming rondom het monster ondersteund wordt en neem hierin mee welke inzichten worden geboden qua vastgelegde informatie, de status van een monster en werkvoorraad van vakgebieden.*

|                 |   |
|-----------------|---|
| Configureerbaar | 3 |
| Out of the box  | 4 |
| Maatwerk        |   |

Beantwoording:

- Een onderzoek wordt voorzien van een onderzoeksnummer. Alle analyses, testen en bevindingen worden onder dit nummer bij elkaar gebracht. Uit te voeren analyses welke bij een bepaald vakgebied horen kunnen als zodanig worden geconfigureerd. Op deze wijze kan een taak bij een of meerdere vakgebieden worden aangevraagd als een vorm van interne ordering. Alle resultaten komen uiteindelijk bij elkaar onder het ene onderzoeksnummer. Een andere partij maakt per monster een zaak aan, dit komt overeen.
- Zaakschermen bevatten duidelijke overzichtsschermen van alle gestructureerde zaakdata, als het ware de metadata van de zaak. Daarbij wordt voorrang gegeven aan inzichtelijkheid in de status van de zaak. Dat

kan, indien gewenst, met behulp van een schematische tijdlijn. Daarnaast geeft de zaakinterface overzichten van de ongestructureerde data (bestanden, foto's).

- Elke zaak is onafhankelijk toegankelijk via werklijsten. Op die manier is het mogelijk werklijsten per vakgebied in te richten en kan het deelonderzoek parallel aan het hoofdonderzoek plaatsvinden.
- Bij binnenkomst vindt registratie van ontvangst plaats in de LIMS door middel van bijvoorbeeld barcode scanning of wordt het monster aangemaakt door de betreffende afdeling.
- Meerdere partijen geven aan dat bevindingen, documenten en (UR) verwijzingen aan het onderzoek kunnen worden gekoppeld.
- Er kan bepaald worden welke informatie of objecten kunnen worden opgeslagen bij het monster of de afzonderlijke analyse.
- Het systeem voorziet in werklijsten waarmee snel inzicht kan worden verkregen in de lopende onderzoeken en het openstaande werk voor de verschillende vakgebieden.
- De hoeveelheid werk binnen een team kan op basis van verschillende parameters geautomatiseerd worden verdeeld. Op basis van de gekozen configuratie instellingen kan de verdeelmodule naar rato het werk verdelen en houdt tevens ook rekening met ziekte en verlof.
- Op elk moment kunnen aanvullende analyses worden toegevoegd die automatisch worden toegekend aan desbetreffend vakgebied.
- Toewijzen samples/subsamples aan verschillende laboratoria tijdens alle fasen van het werkproces. Deze methode wordt ook genoemd door een andere leverancier.
- Definieren verschillende methoden, testplannen e.d. op basis van materiaalkenmerken, klantgegevens, bron e.d.
- Dossiervorming en statusvermelding tijdens alle fasen van het werkproces, wordt door meerdere genoemd.
- Afhandeling en verwerking opdrachten/samples conform 4-ogen principe
- Definitieve afhandeling algemene beoordeling door daartoe gerechtigde verantwoordelijken.
- Material management.
- A powerful search engine available.
- a project can have several tasks.
- Regarding the samples, one dossier can point to multiple samples. A sample is linked to one or several tests (each test is "department dependant", one sample can thus be divided in several subsamples). All the workflow are linked.

*a. Welke zoekmogelijkheden kunnen er worden geboden?*

|                 |   |
|-----------------|---|
| Configureerbaar | 3 |
| Out of the box  | 4 |
| Maatwerk        | 3 |

#### Samenvatting:

Alle partijen geven aan dat er meerdere zoekmogelijkheden in de oplossing zitten.

#### Beantwoording:

- Het systeem voorziet in de standaard overzichten voor filtering en zoek velden waarmee de eindgebruiker eenvoudig door intypen van een tekst filtert in het overzicht en vlot de gezochte objecten in een lijst kan vinden.
- Het systeem voorziet in standaard 'search dialogs' hierin kan de gebruiker aangeven op welk type object of informatie gezocht moet worden. Middels AND en OR filters wordt de zoek actie gericht uitgevoerd.
- Uitgebreide Search-mogelijkheden o.b.v. flexibel gedefinieerde templates van zowel voor stamdata als voor analytische data binnen de functionele modules.
- Voorts zijn er diverse modules waarin nader ingezoomd kan worden op gegevens rechtstreeks vanuit de database maar gepresenteerd worden in een logische / grafische schil welke tevens op maat configureerbaar zijn.
- Eenvoudig een monster terug vinden kan bijvoorbeeld door scannen van een QR- of barcode.
- Alle data in de database kan doorzocht worden.
- Een query window voor hele gerichte en specifieke zoekacties.
- Door twee leveranciers wordt aangegeven dat selecties van search data bewaard kunnen blijven en geëxporteerd kunnen worden.
- Er kan tegelijk op één of meerdere criteria worden gezocht.
- Door de Global (Elastic) Search functie waarmee door alle data in het gehele systeem kan worden gezocht, inclusief bestanden.
- Een oplossing biedt de mogelijkheid om geparametriseerde rapporten te definiëren die invoerwaarden gebruiken om rapportages te genereren. De opgegeven invoerwaarden (parameters) bepalen het bereik (de selectie) van de dataset die te worden getoond in de rapportage. Alle data in het systeem is doorzoekbaar en kan worden gebruikt voor rapportages. Een rapport wordt ook genoemd door een andere leverancier.
- Integrated BI tools (pivot tables, graph views,...).
- Een overzicht van zaken en de benodigde activiteiten per zaak, wordt weergegeven in werklijsten. Werklijsten zijn standaard sorteerbaar, filterbaar en doorzoekbaar. Dat kan op basis van de metadata die per werklijst geconfigureerd kan worden. Werklijsten vormen de standaard toegang tot zaken, elke zaak kan via minstens één werklijst gevonden worden (zelfs de afgesloten zaken, waar geen "werk" meer voor te doen is, zodat "zaaklijst" eigenlijk een betere naam is).
- Inbouwen van extra zoekmogelijkheden o.b.v. de functionaliteit die het DMS daartoe biedt is een mogelijkheid. Binnen of buiten een zaak zou een medewerker hierdoor op een uitgebreidere lijst van metadata (inclusief full tekst search, als het DMS die functionaliteit biedt) naar documenten kunnen zoeken en zo die documenten zelf vinden, of de za(a)k(en) waar ze onderdeel van zijn.

*b. Welke rapportagemogelijkheden kunnen er worden geboden?*

|                 |   |
|-----------------|---|
| Configureerbaar | 3 |
| Out of the box  | 3 |
| Maatwerk        | 1 |

**Samenvatting:**

Alle leveranciers bieden uitgebreide rapportagemogelijkheden.

**Beantwoording:**

- Op het niveau van individuele onderzoeken kan een verslag worden samengesteld dat de resultaten van het onderzoek bevat. De wijze waarop dit verslag wordt samengesteld is configureerbaar. Het resultaat kan worden afgedrukt naar papier, pdf of in de vorm van een elektronisch bestand naar een ander systeem worden verzonden (denk bijvoorbeeld aan een HL7 ORU koppeling). Op basis van de ingevoerde informatie wordt een verslag grotendeels automatisch samengesteld.
- De management module biedt uitgebreide rapportagemogelijkheden en is in feite een BI-tool waarin de database uitgevraagd kan worden. Deze biedt out of the box functies maar is ook configureerbaar en presenteert daarbij de gegevens van de door gebruiker ingestelde parameters. Naast de standaard rapportagemogelijkheden is het altijd mogelijk nog maatwerk toe te voegen aan het systeem.
- Leveranciers van laboratoriuminstrumenten, bieden diverse rapportage tooling binnen hun eigen software suites bij de instrumenten aan. Hier kan de oplossing mee integreren, mits het mogelijk is een gestandaardiseerde koppeling op te zetten zoals bijvoorbeeld op basis van HL7 of XML. Zodoende kunnen we ook met deze data werken en hierover rapporteren. Twee leveranciers benoemen dit.
- De mogelijkheid om in de visual workflows niet alleen werkprocessen en functionaliteiten vlot beschikbaar te stellen aan de gebruiker, maar ook overzichten, tabellen en grafieken/trends te tonen. Hiermee worden intuïtieve dashboards aangeboden waarmee een gebruiker al een vorm van rapportage of overzicht ontvangt.
- Kan rapporten produceren en documentbeveiliging ondersteunen, zowel binnen als buiten de LIMS-omgeving. Elk Pdf document dat door LIMS wordt gegenereerd, kan worden beveiligd om te voorkomen dat het rapport buiten het LIMS-systeem wordt bewerkt of afgedrukt.
- Integratie met Microsoft Office, zodat rapporten moeiteloos kunnen worden geproduceerd met Microsoft Word en Excel zonder dat gegevens van de ene toepassing naar de andere hoeven te worden geëxporteerd en geïmporteerd.

- Geavanceerde grafiek- en trending mogelijkheden, zodat dezelfde rapportindeling kan worden gebruikt voor rapportage in verschillende talen. Versiebeheer van de rapportages is mogelijk met behulp van tussentijdse rapportage en eindrapportage "status" toekenning.
- Geïntegreerde evaluatie functies voor genereren en exporteren van statistische gegevens binnen de LIMS.
- Mogelijkheid om zelf statistische evaluaties en rapportages te maken en beschikbaar te stellen o.b.v. APEX en BIRD.
- Distribueren van evaluaties en rapportages (via mail, printout, webPortal), wordt aangegeven door twee leveranciers.
- Geïntegreerde functionaliteit voor genereren en exporteren van statistische gegevens binnen een webPortal omgeving
- Rapporten kunnen worden opgebouwd uit herbruikbare blokken (sjablonen).
- Rapporten kunnen in elke specifieke lay-out worden gebouwd met alle gegevens uit het systeem (en zelfs externe bronnen indien gewenst).
- Sjablonen voor verschillende rapporten kunnen worden gemaakt en gebruikt om automatisch (PDF-) rapporten te genereren.
- Meertalig rapportagemogelijkheden wordt genoemd door twee leveranciers.
- Alle gegenereerde rapporten kunnen worden afgedrukt en / of opgeslagen onder versiebeheer.
- Met de rapportagetool kunnen rapporten continu worden aangepast en nieuwe indicatoren en grafieken worden opgenomen.
- Gegevens in rapportages kunnen op diverse manieren worden gerangschikt (gefilterd) om resultaten per productie-installatie, per type analyse, per periode (maand/jaar/...), per locatie en/of type operatie te rapporteren. Ook kunnen er met de historische gegevens in het systeem trending-rapporten worden opgesteld.
- Alle individuele testresultaten kunnen worden gecombineerd in één rapportage (bijv. CoA) en ook bij de analyse geplaatste opmerkingen kunnen worden meegenomen in de rapportage.
- Rapportages kunnen automatisch worden verzonden naar emailgebruikers (bijv. aanvragers) en / of gedeeld worden via de klantportal.
- Rapporten kunnen ook direct worden geëxporteerd naar / geupload naar externe systemen.
- De oplossing gaat uit van de inzet van een los commercieel verkrijgbare BI-component, zoals SAS of Business Objects. Aansluiting tussen zaakstelsel en BI-component maakt gebruik van een door het zaakstelsel periodiek of real-time te vullen BI-database. Technische beperkingen van rapportage worden bepaald door de gebruikte BI-component.

3. *Binnen het NRC komt het voor dat een verzameling van monsters op dezelfde manier behandeld worden en hiervoor ook dezelfde administratieve handelingen uitgevoerd moeten worden. Op welke manier ondersteunt de oplossing het batchgewijs werken aan de monsters?*

|                 |   |
|-----------------|---|
| Configureerbaar | 3 |
| Out of the box  | 3 |
| Maatwerk        | 1 |

**Samenvatting:**

Alle leveranciers kunnen batchgewijs werken aan monsters. Er worden diverse mogelijkheden geboden.

**Beantwoording:**

- Het biedt support voor batchgewijs werken per type inzending door gebruik te maken van een ontvangstmodule die geconfigureerd kan worden opdat eventuele repeterende handelingen logisch en vereenvoudigd worden. Ook kan er met bulk invoer of digitaal orderen worden gewerkt voor type inzendingen. De ontvangstmodule kan per type inzending geconfigureerd worden.
- Ja, hier hebben we een specifieke module voor namelijk: batchmanagement. Op een batch of samengestelde hoeveelheid stalen, om een gemeenschappelijke taak uit te voeren. Dit is standaard onderdeel van de LIMS.
- Middels scripting zijn standaard batchgewijze handelingen te configureren en kan de gebruiker de monsters snel en efficiënt verwerken. De well plate readers kunnen bijvoorbeeld op deze wijze ELISA gebaseerde onderzoeken in groter volume met de oplossing verwerken. Door de integratie en daarin het script aan te roepen binnen de oplossing worden de onderzoeken batchgewijs verwerkt binnen de oplossing.
- Een belangrijk hulpmiddel dat hiervoor ingezet wordt is de toepassing van codering (barcodes, 2D codes et cetera).
- Resultaatinvoer wordt uitgevoerd vanuit de onderdelen die analisten dagelijks gebruiken, zoals folders, projecten en batches. Gebruik van folders is de basis waarin monsters worden opgevraagd uit het systeem middels specifieke filters. Vanuit de folder kunnen diverse handelingen worden uitgevoerd als status update, result entry, voorbewerkingen, toevoegen aan een instrument run, etc. De instrument run wordt volledig in de oplossing samengesteld op basis van een template. De template bevat o.a. mogelijkheden definitie van blanco's en standaarden met hun positie in de run. Gezamenlijk uitvoer van de run, communicatie naar instrument, review en validatie is vervolgens mogelijk.
- Verschillende 'Managers' zijn beschikbaar voor groepsgewijs werken met monsters en analyses. De belangrijkste zijn: Folder Manager, Project Manager, Lot Manager, Batch Manager, Investigation Manager, Evidence Location Manager en Werkbladen.

- Integreren en afhandelen en wijzigen van data in batchverwerking.
- Definiëren van templates voor batchgewijs afhandelen van samples.
- Maken van worklists voor instrumenten.
- Een verzameling monsters kan op een werklijst worden geplaatst zodat deze samen door het proces gaan en dezelfde behandeling krijgen.
- Ook is het mogelijk een verzameling monsters te groeperen onder een bepaalde bovenliggende sample, order of batch zodat deze samen door het proces gaan en dezelfde behandeling krijgen.
- Via batchprocessen, dit komt in een aantal situaties voor. Bijvoorbeeld als de zaakinitiatie op een andere plek dan het zaaksysteem heeft plaatsgevonden. Dat gebeurt bijvoorbeeld als via een andere instantie (bijvoorbeeld t.b.v. de uitvoering van een steekproef) de eigenlijke zaakinitiatie in gang wordt gezet. Op basis van een verkregen set gegevens, moeten er gelijksoortige handelingen uitgevoerd worden. Zoiets gebeurt ook als er, bijvoorbeeld wegens tijdsdruk, een voorkant (als een digitaal formulier) live is gezet, om alvast digitale (aanvraag)gegevens in te winnen. Ook bij migraties uit bestaande systemen gebeurt dit. Afhankelijk van de maturiteit van de oplossing, loopt er dan een service over een administratie (of bijvoorbeeld .csv), die één voor één de administratieve handeling uitvoert die uitgevoerd dient te worden. Alle handelingen binnen het zaaksysteem waar geen gebruikersinteractie op plaatsvindt, kunnen door het zaaksysteem beschikbaar gesteld worden als webservice. Als we een monster zien als een zaak en het gaat om het uitvoeren van een administratieve handeling op een verzameling van zaken, maakt zaakgericht werken met een regel gebaseerd systeem een eerder genoemd batchproces overbodig. Gelijksoortige administratieve handelingen kunnen door toevoeging van regels vaak geautomatiseerd worden: diezelfde regels kunnen bepalen voor welke set aan zaken dat geldt. Die processen kunnen zowel synchroon (via een webservice) als a-synchroon (via een zogeheten 'message-event') aangeroepen worden. Dit is iets anders dan klassieke opvatting van batchverwerking (ineens veel data verwerken). Batchverwerking kan met behulp van regels gedefinieerd worden.

4. *Op dit moment kan een binnenkomend monster worden gedeeld binnen het vakgebied en met andere vakgebieden. Dit betekent dat het monster door een vakgebied fysiek wordt opgesplitst zodat andere vakgebieden hierop toetsen kunnen uitvoeren. Kunt u schetsen op welke manier uw oplossing de herleidbaarheid van monsters en daarvan afgeleide sub- en deelmonsters ondersteunt?*

|                 |   |
|-----------------|---|
| Configureerbaar | 3 |
| Out of the box  | 3 |
| Maatwerk        |   |

#### Samenvatting:

Alle leveranciers bieden de mogelijkheden om monsters op te splitsen en ondersteunen de herleidbaarheid hiervan. Hieronder wordt de wijze waarop beschreven.

#### Beantwoording:

- Dit is mogelijk door het splitsen van onderzoeken. Een 1D of 2D barcode zorgt daarbij voor de registratie van het monster en zal gedurende het verloop binnen de workflow aan meerdere vakgebieden kunnen worden voorgelegd. Het aardmateriaal en de verkrijgingswijze als inzending wordt opgeslagen binnen de oplossing. In de oplossing kunnen de acties worden vastgelegd bij het ingezonden materiaal als logische workflow binnen de oplossing, dit kan aan het begin van het proces maar ook later als iemand een aanvullend onderzoek verlangt. Hierbij is zichtbaar dat de vertakkingen aan het onderzoek verder zullen toenemen en kan men gelijktijdig een label printen voor 1D of 2D herkenning van het materiaal. Binnen de Biobank is dit vastgelegd voor studies die een vaste routine volgen binnen de oplossing maar kunnen studies ook worden bijgesteld, waarin bijvoorbeeld een extra tussenstap wordt toegevoegd en zo een nieuwe studie vormt.
- De oplossing is flexibel in de omgang met materiaal(monsters) en in te richten op de wijze waarop NCR zijn monsters en sub- en deelmonsters wil onderzoeken. Daarbij kunnen onderzoeken die gesplitst zijn ook weer worden gekoppeld. Door de inzet van een scankaart (A4 met geautomatiseerd toe te voegen acties) en een handscanner kunnen deze acties makkelijk worden toegevoegd aan de workflow en is een handsfree bediening mogelijk.
- De oplossing ondersteunt aliquots en pool samples. De gecreëerde aliquot of pool monster is uniek geïdentificeerd. De relatie tussen de verschillende monsters en activiteiten wordt volledig vastgelegd en is middels de Genealogie Browser inzichtelijk.
- Sampling/subsampling/opsplitsen van samples vooraf o.b.v. methodedefiniëring of handmatig tijdens alle fasen van het actieve werkproces.
- In het platform zijn processen vrij configureerbaar en gebaseerd op de principes van zaakgericht werken. In geval van het opsplitsen van monsters gaan wij uit van het eerder beschreven principes van hoofd- en subzaken. Waarbij de hoofdzaak het (hoofd)monster betreft en de subzaken de submonster betreffen die via de werklijst per vakgebied door het analyseproces van het betreffende vakgebied worden geleid. Na afronding van de analyses per vakgebied kunnen de resultaten eventueel worden geaggregeerd op het niveau van de hoofdzaak. Door binnen dit mechanisme zorgvuldig om te gaan met het ID/Identificatiecode van het monster en de submonsters is de herleidbaarheid van de sub- en deelmonsters altijd gegarandeerd. Een andere leverancier geeft aan dat hun oplossing ook de mogelijkheid biedt om sub- en deelmonsters te creëren waarbij de hiërarchische relatie in het systeem ten alle tijden behouden blijft. Hiermee biedt de oplossing complete traceerbaarheid en een volledige chain of custody. Voor ieder sub- of deelmonster blijft inzichtelijk (herleidbaar) of deze is afgeleid van een ander sub- of

deelmonster én/of dat er sub- of deelmonster uit zijn afgeleid. Bij het uitvoeren van bewerkingen/handelingen op een batch zullen deze zowel op batchniveau als ook op individueel monsterniveau worden vastgelegd (audit trail).

- One sample is linked to one or several tests. Each test is related to a department. Every test has a lifecycle allowing you to know the status of the sample in each department. If necessary, a full warehouse module is available to track even more precisely to a sample. We are also ready to support feature like RFID to track the samples. The warehouse module allows to track the samples through stock moves and store samples (multi sites warehouse). The solution has a full traceability module associated to the warehouse.

5. *Gedurende het analyse proces staat de precieze aanpak niet vast, maar wordt door de onderzoekers bepaald welke analyses worden ingezet. Op welke manier wordt een dergelijke flexibele workflow ondersteund?*

|                 |   |
|-----------------|---|
| Configureerbaar | 2 |
| Out of the box  | 4 |
| Maatwerk        | 1 |

#### Samenvatting:

Alle leveranciers ondersteunen een flexibele workflow. De inrichting van de flexibele workflow dient wel te gebeuren door de persoon die hier de juiste rechten voor heeft.

#### Beantwoording:

- Alle mogelijke analyses worden in stamtabellen geconfigureerd. Een onderzoeker kan initieel bepalen en vastleggen welke analyses moeten worden uitgevoerd, daarnaast kunnen analyses ten alle tijden als aanvullende of nieuwe analyse aan een monster / onderzoek worden toegevoegd. Aangevraagde analyses komen op relevante werklijsten terecht en volgen hun vooraf geconfigureerd procesflow. Twee andere leveranciers geven ook aan dat alle workflows geconfigureerd kunnen worden.
- Een analist heeft de volledige vrijheid om het proces in te delen als gewenst. Analyses toevoegen of vooraf afsluiten is ten alle tijden mogelijk evenals aanvullen of inkorten.
- Het is mogelijk om intern binnen de afdeling of daarbuiten analyses toe te voegen waarmee ook andere afdelingen kunnen worden aangestuurd. Door middel van aliquots aan te maken kan een deelmonster worden verstuurd naar andere (externe/interne) afdelingen.
- Het zaakstelsel is opgezet in model- en regelgedreven software. In modellen worden regels gemodelleerd. Die regels worden enerzijds gebruikt

voor ondersteuning bij het uitvoeren van activiteiten, anderzijds worden ze gebruikt voor het starten van de juiste activiteiten op het juiste moment. De volgorde van activiteiten wordt daarmee declaratief i.p.v. sequentieel. Dat betekent dat de configuratie van regels bepaalt of en wanneer een activiteit automatisch wordt uitgevoerd, dan wel optioneel handmatig kan worden uitgevoerd, afhankelijk van de informatietoestand van de zaak. Die informatietoestand wordt gevoed door gegevens die al bekend zijn in het informatielandschap van de NRC, of wordt toegevoegd aan de zaak door medewerkers. Afhankelijk van de behoefte van het NRC, kan die workflow dus volledig flexibel worden ingericht. Op deze wijze wordt ervoor gezorgd dat de NRC-medewerker zo min mogelijk handmatige verrichtingen hoeft uit te voeren.

- We have conditions that allows to set triggers to the level of a parameter and if the level is attained, the system will create automatically new parameters and tests to perform.

6. *Binnen het NRC verstaan we onder de Chain of Custody de logging van alle handelingen die gerelateerd zijn aan het monster in de gehele keten vanaf de ontvangst tot de afhandeling van het monster. Op welke manier wordt de vastlegging van de Chain of Custody ondersteund?*

|                 |   |
|-----------------|---|
| Configureerbaar | 2 |
| Out of the box  | 5 |
| Maatwerk        | 1 |

Beantwoording:

- De chain is terug te vinden in de oplossing, waarbij door het aanklikken van de chain ieder stap logisch en herleidbaar is te volgen. Ook kunnen interne transportactiviteiten worden geregeld met een transportmodule voor het verplaatsen van fysieke locatie van het monster.
- Er kan door de onderzoekers informatie worden toegevoegd aan de chain maar dit zal functioneel op maat voor NRC moeten worden vastgelegd in de oplossing, dit omdat ons huidige oplossing nu modulair is ingericht op pathologie en Biobanking.
- Audit Trail & Chain of Custody - Het logging-mechanisme van de oplossing is een continu proces, bewaakt alle activiteiten en wijzigingen en slaat deze activiteiten op met operator-, datum- en tijdgegevens, samen met de vorige waarde en de nieuwe waarde. Voor bepaalde activiteiten zijn redenen vereist en de redenen kunnen worden geselecteerd uit een vooraf gedefinieerde lijst.
- Met de oplossing is het mogelijk om gegevens, zoals een voorbeeld, puur uit de Audit Trail-informatie te reconstrueren. In feite maakt deze zelfde functie het mogelijk om gegevens op elk moment "zoals ze waren" te bekijken, ongeacht het aantal wijzigingen dat sinds die tijd is opgetreden. Audit Trail-informatie wordt opgeslagen voor alle gegevens binnen de oplossing. Dit omvat zowel dynamische gegevens (zoals voorbeelden, tests

en resultaten) als statische gegevens (zoals analyse- en productspecificatiedefinities). Alle configuratie-elementen worden ook volledig gecontroleerd, zoals wijzigingen door bijvoorbeeld triggers. Als een object het ingebouwde versiebeheer van de LIMS gebruikt, is elke afzonderlijke versie op zichzelf staand. Aangezien de Audit Trail een grote hoeveelheid gedetailleerde informatie bevat, is het normaal gesproken noodzakelijk om een subset te zien, zoals wijzigingen in resultaatwaarden of gegevens over de bewaarketen. Met het auditrapportage-element van de LIMS kan elk deel van de Audit Trail worden gerapporteerd om te screenen of af te drukken, waarbij de nadruk ligt op het type of de aard van de wijzigingen. Drie andere partijen geven ook aan dat via audit trails alles traceerbaarheid is en de volledige chain of custody wordt vastgelegd evenals wijzigingen.

- Storage Location Manager ondersteunt opslag en verplaatsingen van monsters binnen de eigen organisatie. Een volledige track & trace van storage locations is hiermee voorzien.
- The solution has a very nice interface to retrieve the informations (messages\_ids at the bottom of the screen). A full audit module is also available. The out of the box messages ids are configured to respect ISO/IEC 17025.
- Het moet altijd duidelijk zijn wie, wat, wanneer, op basis van welke regels heeft gedaan. Van alles wat in het zaaksysteem wordt uitgevoerd, wordt die trace standaard bijgehouden en gelogd. Mochten er voor het NRC extra wensen zijn in de Chain of Custody als het gaat om de vastlegging of ontsluiting van deze gegevens, kan dat ingeregeld/geconfigureerd worden.

7. *Binnen het NRC komen aanpassingen in de werkwijze en methoden voor. Van belang is dat wanneer bijvoorbeeld de methode aangepast wordt het systeem hier ook op aan te passen is. Welke configuratie mogelijkheden worden voor functioneel beheerders en key users geboden?*

|                 |   |
|-----------------|---|
| Configureerbaar | 2 |
| Out of the box  | 3 |
| Maatwerk        | 1 |

#### Samenvatting:

Alle aangeboden oplossingen zijn te configureren en bieden de mogelijkheid om af te wijken en of aanvullingen of aanpassingen te doen (mits dit door een gerechtigden gebeurd).

#### Beantwoording:

- In onze software is het mogelijk om veel hierin te configureren. Dit zouden jullie zelf kunnen doen. We kunnen jullie ondersteunen met scripts, maar we kunnen jullie ook van functioneel beheer voorzien, dat doen we ook voor een aantal andere klanten.

- In de oplossing kan de klant zelf nieuwe modules maken voor specifieke werkzaamheden. Daarnaast wordt er gewerkt aan nieuwe modules waarin nog meer configuratie mogelijk is. Ook de module BioBanking kan hierin voordelen bieden waarbij via scripting specifieke registratiemethoden worden gerealiseerd d.m.v. geautomatiseerd script. Wij willen juist dat de klant zelf zijn onderzoek kan vastleggen vanuit configureerbare modules. Voorzien van de juiste stamgegevens, zoals binnen NRC vastgelegd kan een key user het onderzoek vastleggen als logische workflow binnen de oplossing. De insteek hierbij is dat voor 90% NRC's key users de workflow voor nieuwe onderzoeken kunnen inrichten en voor de overige 10% de leverancier ondersteunt middels scripting (opgevolgd in een nieuwe versie).
- Alle objecten / templates zijn onderhevig aan versie beheer. Een volledige audit trail op deze template is aanwezig in de LIMS. Audit Trail-informatie wordt opgeslagen voor alle gegevens binnen de LIMS. Dit omvat zowel dynamische gegevens (zoals voorbeelden, tests en resultaten) als statische gegevens (zoals analyse- en productspecificatiedefinities). Alle configuratie-elementen worden ook volledig gecontroleerd, zoals wijzigingen door bijvoorbeeld triggers. Als een object het ingebouwde versiebeheer van de LIMS gebruikt, is elke afzonderlijke versie op zichzelf staand.
- Door de snelle en effectieve mogelijkheid om entiteiten te kunnen configureren (en de mogelijk om proces specifieke workflows op te zetten (de Process Stations) kan het systeem eenvoudig en snel worden aangepast. Daarbij wordt versiebeheer en de audit trail van de gebruikte dataformulieren ook volledig ondersteund.
- The adaptations are recorded in the system. All adaptations are also submitted to specific right of access. The system will automatically adapt itself when a change is approved. Relatief eenvoudige en snelle aanpasbaarheid is juist de grote kracht van het platform. Het platform beschikt over modelgedreven software om zaaksystemen snel en eenvoudig op maat te kunnen modelleren. Deze modellen worden 1 op 1 geëxecuteerd in de runtime(s). De ingerichte processen en methodes kunnen dan ook volledig naar behoefte aangepast worden. In de model-rechtenstructuur is toekenbaar welke elementen er door bepaalde gebruikers ingezien dan wel aangepast mogen worden. Als functioneel beheerders en/of key users de juiste opleiding hebben gehad, zijn zij in staat om die modellen in de modelleeromgeving van de oplossing te wijzigen en daarmee de gewenste functionaliteit aan te passen.

8. *Het NRC is ISO 17025 gecertificeerd. Op welke manieren ondersteunt uw oplossing deze ISO 17025 certificering?*

|                 |   |
|-----------------|---|
| Configureerbaar | 2 |
| Out of the box  | 5 |
| Maatwerk        | 1 |

Beantwoording:

- De oplossing wordt momenteel bij alle vooraanstaande labs ingezet voor de verslaglegging van alle onderzoeksgegevens. Daarbij worden deze labs getoetst op de ISO 15189. Een norm die qua cross reference redelijk vergelijkbaar is met die van de ISO 17025 echter toegespitst op medische laboratoria. Inhoudelijk is de ISO 15189 breder ingestoken en legt meer nadruk op het totale proces (pre-analyse | analyse | post analyse) dan meting en resultaat alleen. Het gaat om de totale service die laboratoria biedt van aanvraag tot/met rapportage. Logisch dat onze oplossing dan ook aansluit bij de medische professie die binnen deze labs als taal/jargon wordt gehanteerd.
- De compliancy voor ISO17025 wordt ondersteund met de standard Document Management, Training Management, Investigation Management and Uncertainty Measurement mogelijkheden.
- Een volledig functionele ISO17025 Component Template is beschikbaar om uw lab volledig op ISO17025 te ondersteunen. Een component template omvat out-of-the-box functionaliteit direct inzetbaar en in te richten.
- Versie gecontroleerde analytische stamdatabeheer.
- Versiebeheer van stamdata.
- Samplebeheer.
- Kalibratie o.b.v. regelkaarten.
- Gebruiksvoorwaarden voor chemicaliën.
- Toewijzing van gebruikersrechten o.b.v. gebruiksprofielen.
- ISO17025 conforme distributie van berichten en archivering.
- De software bevat alle elementen (functionaliteiten) om te kunnen voldoen aan ISO 17025. Door validatieregels te configureren en doordat gegevens direct real-time beschikbaar kunnen worden gemaakt, wordt data-dubbeling voorkomen. Ook kan er batchgewijs data worden geregistreerd, kunnen uitslagen conform ISO-17025 eisen worden gegeneerd, worden alle wijzigingen in het systeem geautomatiseerd geregistreerd in een overzichtelijke audit trail. Het gebruik van audit trails wordt ook aangeboden door een andere leverancier. Daarnaast kan per verrichting /test/resultaattype in de oplossing met eenvoudige configuratie worden aangegeven of het wél of geen geaccrediteerde test betreft. Het kwaliteitskenmerk "onder accreditatie (ISO 17025)" kan ook op rapportages worden vermeld bij de betreffende onderdelen.
- Twee leveranciers geven aan dat het ook geen probleem is om het systeem aan te passen aan de eisen en wensen van de NRC.
- The solution is compliant regarding security and integrity of the data. Regarding the LIMS, it is developed in accordance with the requirements of the ISO/IEC 17025.
- De oplossing zorgt ervoor dat alle informatie met betrekking tot de te analyseren monsters binnen de BVMA samenkomt en altijd actueel raadpleegbaar, traceerbaar en herleidbaar is. Op deze wijze kan de betrouwbaarheid en de kwaliteit worden aangetoond.
- Daarnaast is het mogelijk om in onze oplossing de relevante meetpunten van de standaard zelf vast te leggen. Op zodanige wijze dat de acties die in het kader van de naleving worden uitgevoerd in het BVMA kunnen worden vastgelegd. Denk aan een planning voor apparatuur onderhoud en

kalibraties, met meldingen/notificaties voor wanneer actie vereist is en een mogelijkheid om de uitvoering hiervan te loggen. Bij audits kan op deze wijze snel aangetoond worden dat het laboratorium compliant is.

9. *Kunt u schetsen wat uw visie is ten aanzien van de door uw aangeboden oplossing?*

Beantwoording:

- Met in achtname van het door de NVWA en de NRC gestelde uitgangspunten kan de oplossing worden aangepast en ingericht. Met eigen specialisten en met kennis en ervaring binnen de vakgebieden zijn we in staat om een passend LIMS te implementeren volgens afgesproken kaders. Gemiddeld zijn we 6-9 maanden bezig om een nieuwe LIMS te implementeren. Gelet op dat het project een uitgebreide functionele analyse verlangt en waarbij er veel gegevens op papier zijn vastgelegd binnen de diverse werkgroepen, mag er zeker nog 3 maanden bij opgeteld worden. Dit omdat deze functionele fase tevens vertaald moet worden naar de inrichting en scope van de LIMS. Vanuit de ontvangen documenten die betrekking hebben de aanschaf van een LIMS kan worden gesteld dat 40% configurabel en de overige 50% out of the box en 10% maatwerk. Kortom een project waar veel wordt gevraagd aan een leverancier/system integrator! En er korte lijnen zijn met de diverse disciplines die een dergelijk project verlangen veel van de leverancier.
- We maken gebruik van state-of-the-art technologie die is gebouwd op een platform dat naadloze modulaire implementatie van functionaliteit aan klanten mogelijk maakt, gebruikmakend van onze unieke aanpak in de branche om de levensduur en uitbreidbaarheid van al onze klantensystemen te garanderen.
- We maken het laboratorium efficiënter door het digitaliseren en automatiseren van de werkprocessen in en rond het laboratorium en ontlast laboratorium medewerkers van routinematige bezigheden.
- Met onze oplossing bieden wij één platform voor complete laboratorium automatisering. Uitgangspunt is om één flexibele gestandaardiseerde totaaloplossing te bieden voor laboratoria en onderzoeksinstituten in zeer uiteenlopende branches. In het platform is alle functionaliteit aanwezig voor de configuratie van LIMS, ELN, LES, SDMS en andere laboratorium applicaties. Het is onze ambitie om met het geavanceerde Platform voorop te blijven lopen in de laboratoriumautomatiseringsmarkt door continue in te spelen op nieuwe technologische ontwikkelingen. Daarbij wordt er o.a. gebruik gemaakt van geavanceerde web en mobiele technologieën waardoor ons systeem gebruikt kan worden op alle mobiele apparaten waar en wanneer ter wereld. Onze unieke aanpak kenmerkt zich o.a. door de continue integratie (continuous delivery) van nieuwe functionaliteiten en het bieden van gratis (automatische) upgrades/updates waarmee er geen sprake meer is van maatwerk, dure en langdurige upgrade projecten en/of functionele achterstanden.

We willen graag samen met de NVWA een langdurige samenwerking opbouwen waarin het platform kan worden doorontwikkeld en binnen de NVWA verder kan worden uitgerold.

- We are the most complete solution on the market. We have around 40 main modules and a store of more than 20k apps. In the case of an institute like yours, links with applications as the project module is an asset. If you look at the LIMS, the solution is very complete. If you look at the other modules, it is always full featured modules. There is an almost infinite possibilities of enhancing functionalities of the system.
- Wij denken dat het voor de ontzorging van de NVWA relevant is een partij te kiezen die voldoende kennis en ervaring heeft in zowel het domein van de laboratoria als de overheid.

## 1.2 Dienstverlening

10. Kunt u aangeven welk(e) scenario(s) (zie paragraaf 3.4) u resultaatverplicht kunt leveren en op welke wijze?

Samenvatting:

| <b>Scenario</b>                             | <b>Aantal</b>                                                 | <b>Opmerkingen</b>                                                                                                                       |
|---------------------------------------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| 1.SAAS oplossing                            | <i>1 plus 1 keer minder geschikt</i>                          | <i>2 keer wordt aangegeven niet geschikt</i>                                                                                             |
| 2.Outsourcing bij System Integrator         | <i>5, waarvan 1 een duidelijke voorkeur voor dit scenario</i> |                                                                                                                                          |
| 2a. System Integrator + IaaS / Paas         | 3                                                             |                                                                                                                                          |
| 3.Twee kavels: pakket en System Integrator  | <i>3, waarvan 1 een duidelijke voorkeur</i>                   | <i>1 van de 3 geeft aan dit niet resultaatverplicht te kunnen leveren</i>                                                                |
| 3a. DICTU + Pakket                          | 5                                                             |                                                                                                                                          |
| 3b. System Integrator + IaaS/ Paas + pakket | 5                                                             |                                                                                                                                          |
| 4.Zelf doen                                 | 4                                                             | <i>1 van de 4 geeft aan dat het minder voor de hand ligt. Een andere partij geeft aan via inzet low code platform (Mendix, Powerapps</i> |

Beantwoording:

- In aanvulling op bovenstaande tabel geeft een leverancier ook aan de hosting op verschillende manieren te kunnen leveren. Hosting in a cloud of your choice (NRC contract with a provider of your choice/Hosting on premises.

- Een volledige SaaS-oplossing (variant 1) biedt naar verwachting onvoldoende mogelijkheden om de 8 verschillende vakgebieden op specifieke wijze te ondersteunen en de vergaande digitaliseringsbehoefte in te vullen. Dit wordt door een andere leverancier bevestigd die aangeeft dat ze een SaaS oplossing leveren voor verschillende markten. Echter rekening houdend met de processen en eisen/wensen binnen de NVWA project verwachten wij dat uw bedrijfsproces niet geschikt is voor een typische SaaS oplossing.
- In het geval van het SAAS scenario zien we een zorg. Wanneer we volledig naar een cloud omgeving gaan, dan heb je verschillende cloud omgevingen naast elkaar draaien. Complexiteit infrastructuur wordt groter en de kosten worden hoger.
- Het splitsen van de dienstverlening in twee kavels waarbij de NVWA of een andere leverancier (variant 2a en 3b) zelf een apart IaaS/PaaS contract afsluit biedt in onze visie geen extra voordelen en minder mogelijkheden om te profiteren van de schaalvoordelen die onze oplossing biedt.
- Ook variant 3a (DICTU+Pakket) zien wij als een goede mogelijkheid om de doelstellingen van de NVWA te realiseren. DICTU treedt op als ICT-leverancier van de NVWA en wij installeren de oplossing binnen de DICTU Cloud. Daarnaast verzorgen wij functionele inrichting en de integratie binnen het applicatielandschap en de architectuur van de NVWA. Dit kan desgewenst resultaatverplicht uitgevoerd worden.
- Wij ondersteunen scenario 2 (nog) niet. Hierbij ligt de outsourcing bij de system integrator. Wij werken met name voor ziekenhuizen en in een ziekenhuis staat veiligheid voorop. Hierdoor is binnen een ziekenhuis vaak de IT omgeving of een andere system integrator verantwoordelijk voor het aanbieden van een oplossing in een datacenter. Wij zijn gewend om met al die partijen af te stemmen. We zijn nog niet eerder gevraagd om deze rol te vervullen.
- Onze algemene aanpak van LIMS implementaties. Wij werken volgens de best practice van Prince2. Medewerkers zijn getraind en gewend om in deze structuur te werken. Dit is niet om zomaar 'blind' alle processen en componenten van Prince2 uit te voeren maar wel om te bekijken wat er in de specifieke situatie bij de klant benodigd is. Een en ander geschiedt altijd in goed overleg met de klant. We starten altijd vooraf met een gesprek met de feitelijke opdrachtgever bij de klant (wie vervult deze rol en heeft ook het mandaat om dit te mogen doen) over de opdracht en de projectorganisatie-structuur, waaronder de projectleider aan de kant van de klant. In de voorbereiding van de aftrap van het project verzetten alle projectdeelnemers en interne (en wellicht externe) betrokkenen relatief veel werk. Hier geldt dat een goede voorbereiding het halve werk is. Met deze nauwgezette voorbereiding willen we een ieder van tevoren duidelijkheid geven over: De op te leveren producten en diensten binnen het project;  
 Hoe deze producten binnen logisch gekozen productgroepen geclusterd worden;  
 Hoe die productgroepen ook in logisch gekozen werkgroepen dienen te worden opgepakt;

De te bereiken mijlpalen in de tijd;

De inrichting van het project met de beschrijving van de gezamenlijke project organisatie structuur met daarbinnen:

1. Een stuurgroep (met de verschillende rollen die in een stuurgroep moeten zijn belegd, zoals de opdrachtgever, de senior user - degene die beoordeelt of de opgeleverde producten en diensten geaccepteerd kunnen worden - en de senior suppliers, waaronder vaak een ICT-manager, een lab-manager en een manager van ons).
2. Werkgroepen, meestal bestaande uit een technische werkgroep en een functionele werkgroep, een werkgroep die de dataconversie uitvoert en een werkgroep die de trainingen verzorgt en de communicatie verzorgt;
  - Wat in de scope en wat buiten de scope valt.
  - Een product breakdown structure (PBS) en een meer gedetailleerd niveau in een work breakdown structure (WBS);

Er is veel praktijkervaring bij verschillende klanten met de implementatie van de oplossing, waarbij we het gulden midden bewaren tussen goed gestructureerd werken maar niet bureaucratisch werken. In de dagelijkse aansturing van het project stuurt de projectleider van de klant samen met de projectleider van de leverancier op een pragmatische en efficiënte manier op de realisatie van de projectdoelstellingen, zonder op de kracht van bovenstaande in te boeten.

- Bij scenario 2 ligt de outsourcing bij de system integrator. Wij werken met name voor ziekenhuizen en in een ziekenhuis staat veiligheid voorop. Hierdoor is binnen een ziekenhuis vaak de IT omgeving of een andere system integrator verantwoordelijk voor het aanbieden van een oplossing in een datacenter. Wij zijn gewend om met al die partijen af te stemmen. We zijn nog niet eerder gevraagd om deze rol te vervullen.

*11. In geval van scenario 1 (SaaS), kunt u daarbij aangeven hoe u omgaat met het einde van de contractperiode, waaronder het terug leveren van data en het opruimen van de voor de NVWA ingerichte omgeving?*

Beantwoording:

- Meerdere leveranciers geven aan dat de data wordt overgedragen aan de NVWA. Vervolgens wordt de data van de NVWA door de leverancier vernietigd. De NVWA blijft eigenaar van de data, dit is ongeacht of de data in een cloud situatie staat of on-premise.
- Na beëindiging van een contract is de leverancier gehouden om mee te werken de data in een of andere vorm (meestal in de vorm van exportbestanden) over te dragen aan de opdrachtgever opdat de data in een nieuw systeem kan worden geïmporteerd. Afspraken hierover worden op hoofdlijnen vastgelegd in een exitplan als bijlage bij de overeenkomst. De details kunnen pas worden uitgewerkt op het moment dat de situatie zich voordoet omdat vele factoren de praktische uitwerking beïnvloeden.
- In geval van een virtuele inrichting wordt de data vernietigd volgens een overeengekomen Wipe procedure geschoond. Daarbij hanteren we de door de NVWA minimaal gestelde procedure.

- In een retransitieplan worden specifieke afspraken rondom onder andere het terug leveren van de data en het verwijderen van de specifieke NVWA omgevingen en gegevens beschreven. De oplossing zelf blijft eigendom van de leverancier.

*12. Heeft u suggesties voor een andere verdeling van de elementen waar een dienstverleningsscenario uit is opgebouwd waardoor u beter in staat bent om in te schrijven of mist u essentiële elementen in de verschillende dienstverleningsscenario's?*

Samenvatting:

Een aantal leveranciers geven aan geen suggesties te hebben, van de anderen hieronder de aanvullingen.

Beantwoording:

- De voorkeur ligt bij scenario 3. Dit omdat het aspect randapparatuur niet vergeten moet worden. De integratie van randapparatuur is voor een laboratorium van cruciaal belang en dient er rekening te worden gehouden met de volledige inrichting van het lab. Ook het toekomstperspectief is hierbij van belang. Nieuwe onderzoeksmethodes en apparatuur zal zijn intrede krijgen. De domeinen dienen dan ook dusdanig te zijn ingericht dat de omgeving schaalbaar en flexibel is maar wel vanuit een duidelijke standaardisatie en inrichting. De oplossing werkt volledig op Microsoft producten waaronder ook Azure. Maar ook voor wat betreft werkplekinrichting en gekozen database architectuur. Het is dan ook zinvol om op tijd een architect te betrekken voor een goede afbakening van de domeinen.
- Kan o.b.v. een inspanningsverplichting tevens de overige scenario's 2 en 3b ondersteunen waarbij de leverancier het primaire aanspreekpunt is.
- In principe is de opdrachtgever (NVWA) verantwoordelijk voor het functioneel en applicatiebeheer (zoals, maar niet beperkt tot, het beheer van gebruikersaccounts en gebruikersrechten, configuratie, gegevensinvoer, berichtenverkeer etc.), en het beheren en verstrekken van (technische) documentatie. Het LIMS pakket wordt geleverd met uitgebreide ondersteuning en de leverancier is verantwoordelijk voor de ontwikkeling en de Support van de oplossing.
- Bij scenario vier missen we nadrukkelijk het uitbesteden van software ontwikkeling en beheer van een low code "maatwerk" LIMS ontwikkeling.
- I have a remark regarding the do it yourself. A full LIMS system took us several tens of thousands hours to develop. I would also recommend to be careful with that option because you will have to prove the compliance with the norm and the associated more local requirements.

### **1.3 Architectuur en data**

*13. Past uw LIMS-oplossing binnen het in paragraaf 3.4 beschreven beoogde componentenlandschap van de NVWA en op welke wijze?*

#### Samenvatting:

Alle leveranciers geven aan dat de oplossing past binnen het componenten-landschap van de NVWA. Enkele beschrijven ook de wijze waarop, zie hieronder.

#### Beantwoording:

- Ja, de oplossing kan op verschillende wijzen worden geïmplementeerd die volledig aansluiten bij de enterprise architectuur. De oplossing is zeer connectief en kan met verschillende communicatie brokers of servicebus communiceren. De LIMS kan indien connectiviteit is geregeld ook domein overstijgend functioneren. Voor het uitwisselen tussen systemen is tot op heden LIMS nooit de beperkende factor geweest.
- Voor LIMS vereist een applicatieserver en MS SQL database al dan niet op een cluster. De gebruikers starten de executabel van LIMS vanuit de werkplek, dit kan ook vanuit de packaging.
- In geval van volledige outsourcing, baseert de leverancier de oplossing op het platform dat wordt gehost op de Azure cloud infrastructuur van de system integrator. In geval van hosting binnen DICTU of bij een andere partij baseren wij onze oplossing voor de BVMA op één of meerdere componenten van ons platform. Uitgaande van scenario 2, biedt dit platform een set geïntegreerde herbruikbare bouwblokken/softwarecomponenten die op basis van open standaarden en API's op gestandaardiseerde wijze zijn gekoppeld. Koppelbaarheid van het platform met andere systemen en bronnen (registers en administraties) op basis van gangbare standaarden is standaard voorzien in de open architectuur van het platform. Het platform biedt dan ook "by design" uitstekende mogelijkheden om de koppelingen te realiseren.

Voor de realisatie van de benodigde koppelingen met de registers en administratie maken wij gebruik van de integratiecomponent van het platform. Deze Cloud SaaS-oplossing biedt een veilige en robuuste centrale koppeldienst en aansluitpunt voor overheden, bedrijven en Landelijke Voorzieningen. De integratiecomponent voorziet onder andere in de volgende functionaliteiten:

- Centraal Aansluitpunt voor ebMS- en WUS- (digikoppeling) dataverkeer ten behoeve van de ontsluiting van de Basis- en Kernregistraties cq. Landelijke Voorzieningen.
- Diginetwerk (overheidsnetwerk) voor berichtenverkeer met het RvIG (BRP/GBA-V).
- API-Management.
- Servicebus voor koppelen van zowel interne- als externe (Domein) applicaties via REST of SOAP webservices.

De oplossing is met één "stekker" (technisch koppelvlak) geïntegreerd binnen het platform en verzorgt op uiterst veilige en betrouwbare wijze de benodigde koppelingen tussen de BVMA en de applicaties, registers en administratie binnen het NVWA componenten landschap. De NVWA kan op deze wijze met een beveiligde verbinding en beveiligde berichtenstromen gegevens met elkaar uitwisselen conform de landelijk geldende overheidsstandaarden. De koppelingen met de landelijke voorzieningen (zoals de basisadministraties) zijn overigens standaard in onze oplossing voorzien. Het platform kan voorzien in zijn eigen

administratie voor het beheren van de proces/transactie gegevens binnen de BVMA, maar kan ook gebruik maken van de bestaande (monster)administratie en zaakadministratie binnen het componentenlandschap van de NVWA. De opslag van documenten en hun metadata vindt plaats via de CMIS-standaard binnen het DMS. Ook hier geldt dat de documenten kunnen worden opgeslagen in het DMS van het platform, maar ook in de Documentadministratie van de NVWA. Voor de koppelingen tussen de LIMS-applicatie en andere NVWA applicatie(s) kan eventueel ook rechtstreeks (zonder tussenkomst van de service bus) met webservices worden geïnteracteed.

*14. Ondersteunt uw LIMS-oplossing het uitwisselen van data en welke uitwisselstandaarden hanteert u daarbij?*

**Samenvatting:**

De uitwisseling van data wordt door alle leveranciers ondersteund en de standaarden xml, csv en APOI's worden door meerdere benoemd.

**Beantwoording:**

- De uitwisseling van data met andere systemen wordt ondersteund. Wij hebben ruime ervaring met HL7 standaarden, xml, .csv. voor andere uitwisselvormen is maatwerk ontwikkeling mogelijk.
- We offer a open source solution and the exchange of data is very convenient (web services, REST API).
- De door ons aangeboden LIMS wordt vaak gebruikt om te communiceren met bijvoorbeeld laboratoriuminstrumenten, Process Information Management Systems / Manufacturing Execution Systems (PIMS / MES) en ERP / SAP. We ondersteunen alle populaire gegevensuitwisselingsformaten, waaronder CSV, XML, Webservices, directe databasetoegang (SQL/ ODBC/ JDBC), API's, externe functieaanroepen (RFC's), OLE Automation, OLE for Process Control (OPC), ActiveX, FTP, TCP/IP Sockets, e-mailberichten (SMTP/ MAPI/ VIM), RS-232 seriële communicatie, LabStation, ASTM/HL7 protocollen, etc. Sommige van onze klanten gebruiken middleware-producten om onze LIMS aan te sluiten op andere toepassingen.
- We bieden een compleet framework voor (geautomatiseerde) gegevens-uitwisseling tussen verschillende (interne/externe) systemen/laboratoria/onderzoeksinstituten (o.a. voor het uitwisselen van opdrachten, studies, monsters en resultaten). En beschikken over zeer uitgebreide koppelmogelijkheden met externe systemen en het team beschikt over een zeer ruime ervaring en expertise op het gebied van koppelingen met externe databases/systemen (o.a. ERP, MES, CRM, ....). We beschikken over de volgende standaard componenten:
  - Web-API - Set of web functies that can be used to exchange data.
  - Service process (database) – Service application that runs task based on events or time schedule.
  - Agent (internet) – Windows application connected with the LIMS to automate tasks.Daarnaast beschikt de oplossing over de volgende standaardfuncties:

- External Record – Mechanism to define that a record is owned by an external system.
  - Mapping System – Manage names of entities as they are named in other systems for translations.
  - Task runner – Background task that can import data from WebResources, FTP and/or File System .
  - XML – Data import and export.
- Ondersteunt data uitwisseling o.b.v. gedefinieerde interfaces voor Webservices, API 's en File Based Transfer.
  - Onze oplossing voor LIMS, gaat uit van het principe 'interoperability by design'. Door uit te gaan van de 'pas toe of leg uit-lijst' van het Forum Standaardisatie zorgen wij ervoor dat het platform maximaal aansluit op de standaarden voor integratie die gelden binnen de Nederlandse overheid. De onderliggende Platformstrategie van het Platform is hierin essentieel. Het platform is opgebouwd uit een set geïntegreerde herbruikbare bouwblokken/softwarecomponenten die op basis van open standaarden en beveiligde API's op gestandaardiseerde wijze zijn gekoppeld. Door binnen het platform vast te houden aan deze strategie borgen wij dat de componenten eenvoudig kunnen worden vervangen door een nieuwe component die wordt geïntegreerd met behulp van binnen de Nederlandse overheid gebruikte open standaarden
  - Het platform biedt uitstekende mogelijkheden om de (data-) bronnen/registers, administraties en applicaties te koppelen en ontsluiten en integratieproblemen te voorkomen. De toegangs- en integratiecomponent spelen hier een belangrijke rol bij.

Een aantal voorbeelden van standaarden die wij ondersteunen:

- REST en SOAP voor webservices.
- CMIS voor documentbeheer.
- Digikoppeling, ebXML voor betrouwbaar berichtenverkeer tussen overheden.
- SAML2.0 en Oauth voor toegangsverlening.

*15. Ondersteunt uw oplossing Single Sign On en zo ja, volgens welke standaarden?*

Samenvatting:

Op 1 leverancier na ondersteunen alle oplossingen Single Sign on.

Beantwoording:

- Als leverancier gaan we uit van een 2-factor authenticatie waarbij de toegang tot het werkstations veelal door een token of login wordt geborgd. Toegankelijkheid van de LIMS hangt samen met de rol die de persoon heeft in de LIMS en daarom dient specifiek nog in LIMS te worden ingelogd.
- Ja, SAML 2.0 wordt ondersteund.

- Ja, Single Sign On wordt ondersteund. Wij hebben o.a. ervaring met de volgende standaarden: Security Assertion Markup Language (SAML) and Web Services Federation (WS-Fed).
- SSO oplossing "Aangemelde Windows gebruiker" en Lightweight Directory Access Protocol (LDAP)/ ActiveDirectory authenticatie.
- Voor de Webinfo (webPortal oplossing) kan Kerberos-authenticatie worden gebruikt (Kerberos 5 met SPNEGO, RFC 4559).
- Twee leveranciers geven aan dat klantspecifieke aanpassingen op aanvraag mogelijk zijn.
- Er wordt gebruik gemaakt van de volgende standaarden; LDAP, OAuth Authentication, Google Authentication
- Voor het inloggen met SSO wordt gebruik gemaakt van een Identity Broker. Deze oplossing vormt de Toegangscomponent van het Platform. De Identity Broker kan worden aangesloten op IDP/Ident van de NVWA. Een medewerker die van zijn werkplek naar LIMS navigeert wordt "onder water" via de Identity-broker geauthentiseerd. Na succesvolle authenticatie wordt de gebruiker naar het juiste Dashboard doorgeleid. Met deze aansluiting op SSO beschikt de LIMS-applicatie over een gebruiksvriendelijk en bewezen oplossing voor toegangsverlening van uw medewerkers.
- Bij hosting van LIMS binnen de DICTU Cloud zullen wij naar verwachting rechtstreeks koppelen met TVS (het ToegangsVerleningSysteem) en IDP/Ident. Hierbij kunnen we naar verwachting gebruik maken van bewezen koppelingen.

*16. Welke voorzieningen biedt uw oplossing voor het inrichten van toegangsbeveiliging (autorisaties)?*

Beantwoording:

- De autorisaties van de gebruiker binnen de oplossing worden geconfigureerd op basis van de functie/rol van de gebruiker in combinatie met het procesonderdeel waar de gebruiker actief is.
- De instellingen kunnen door de functioneel beheerder worden geconfigureerd, passend bij de door de NVWA opgelegde password criteria.
- De oplossing biedt twee soorten wachtwoorden voor elk gebruikers-account: inlogwachtwoorden en ondertekening wachtwoorden. Het aanmeldingswachtwoord wordt gebruikt om de identiteit van de gebruiker te verifiëren tijdens het inloggen op het systeem, het ontgrendelen van het systeem en tijdens gebruikersbevestigingsprompts in het hele systeem. Het ondertekening wachtwoord wordt uitsluitend gebruikt om elektronische handtekeningprompts in te vullen.
- De oplossing ondersteunt de optie om Windows-referenties te gebruiken om LIMS automatisch te starten. Het webequivalent van Windows-aanmelding is SSO.
- De oplossing biedt de gebruiker een mechanisme om de gebruikerssessie te vergrendelen zonder zich af te melden bij de toepassing.

- De LIMS integreert met LDAP in vijf functionele elementen: LDAP-authenticatie, User field mapping, LIMS-rollen, Automatisch aanmaken gebruikers en LDAP-Credential Caching. Nadat het gebruikersaccount is geverifieerd op LDAP, evalueert het systeem de LDAP-server voor geconfigureerde LIMS-rollen. Als het gebruikersaccount is geconfigureerd met rollen in LIMS, worden deze rollen gebruikt en worden LDAP-rollen genegeerd. Als de gebruikersaccount in LIMS geen rollen heeft gedefinieerd en is geconfigureerd voor het gebruik van rollen, worden rollen gebruikt die zijn gedefinieerd op het LDAP-account.
- De LIMS ondersteunt functionaliteit om gebruikers na bepaalde tijdsintervallen af te sluiten. Bovendien kan LIMS de sessie van de gebruiker sluiten.
- Iedere gebruiker heeft zijn eigen login account en wachtwoord. De oplossing biedt uitgebreide mogelijkheden voor wachtwoordbeheer: Active Directory, Active Directory Federation Services (ADFS) indien gewenst, multi-factor authenticatie, en afdwingen van complexe wachtwoorden die standaard na 90 dagen verlopen (configureerbaar).
- De veiligheid en beveiliging van opgeslagen geheime en vertrouwelijke informatie wordt gewaarborgd door een strikt toegangs- en wachtwoordbeleid, de validatie van gegevens en invoer, het gebruik van encryptiemethoden, het gebruik van audit trails en het ontwikkelen en onderhouden van de software volgens de SDLC methode.
- Het platform is een gesloten systeem. Secure Sockets Layer (SSL) - codering wordt gebruikt om gegevens te versleutelen die worden verzonden tussen de clientinterface en de centrale server. SSL breekt ieder bestand in zeer kleine datapakketten. Deze datapakketten worden versleuteld voordat ze worden verzonden. Bij het ophalen van de datapakketten worden deze gedecodeerd en opnieuw samengesteld. Alle gegevens worden dus in een gecodeerde indeling verzonden zodat ongeautoriseerde gebruikers de oorspronkelijke gegevens niet kan inzien. Alle wachtwoorden worden ook opgeslagen in een 'hashed' en 'salted' indeling in de database. De SSL-codering wordt uitgevoerd binnen de protocollaag en is beschikbaar voor alle SQL Server-clients.
- Geïntegreerde module voor toewijzing van gebruikersrechten op basis van gebruikersprofielen.
- Maakt gebruik van een gecertificeerd Europees Datacenter voor de SaaS oplossing
- Access rights are configured per user/group of user per module (several roles per module), per specific action, per model, per field. The solution allows you to use a double id system (by email, sms).
- Het platform biedt een component voor toegangsverlening. Deze component verzorgt de identificatie en authenticatie van alle gebruikersgroepen binnen de LIMS op basis van een Identity as a Service Concept. De oplossing is gebaseerd op de SaaS Identity-broker oplossing en is al geïntegreerd binnen de oplossing. Het zorgt dat alle gewenste inlogmiddelen (denk aan DigiD, eHerkenning en SSO) binnen LIMS gebruikt kunnen worden.
- Het platform biedt zowel rol- als attribuut gebaseerde autorisatiemogelijkheden. Een functioneel beheerder kan per

gebruikersgroep/gebruiker autorisaties en functionaliteiten toewijzen of intrekken. Autorisaties worden fijnmazig aan een rol gekoppeld, zowel op het niveau van processen als op het niveau van toegang tot gegevens. Op deze wijze krijgen alle gebruikers afhankelijk van hun rol/kenmerken functionaliteiten aangeboden en wel of geen inzage in (delen van) het dossier en de onderliggende gegevens.

*17. Welke processen hanteert u om de kwaliteit van uw softwareproduct te borgen? Denk hierbij aan aspecten uit de ISO 25010 standaard?*

Samenvatting:

Alle leveranciers hebben een beleid of proces beschreven om de kwaliteit van de software te borgen. De inhoud van dit beleid of proces is divers.

Beantwoording:

- Het softwareontwikkelproces is opgezet op basis van een beleid voor beveiligd ontwikkelen. De verschillende onderdelen van het proces, zoals ontwerp, ontwikkeling en testen worden conform een gestructureerd proces uitgevoerd dat periodiek wordt geëvalueerd.
- Door een goed gedefinieerd productontwikkelingsproces, waarvoor er een volledige set standaard operating procedure (SOP's) is en er kwaliteitshandboeken zijn die het proces van productontwikkeling tot productrelease beschrijven. Deze SOP's zijn:
  - H01 Backups and Disaster Recovery Procedure.
  - H02 Development Life Cycle Procedure.
  - H03 Product Release Procedure
  - H04 Programming Standards Procedure
  - H05 Change Control Procedure
  - H06 Audit Procedure
  - H07 Product Shipment Procedure
  - H08 Change Management Procedure
  - H09 Training Material and Course Administration
  - H10 Customer Support Procedure
  - H11 Team Member Training and Certification Procedure
  - H12 Style Guide Procedure
  - H13 IT Equipment and Security Procedure
  - H14 Product Release QA Procedure
  - H15 Customer Notification Procedure
  - H16 Internal QA Systems Management Procedure
  - H17 Document Management Procedure
  - H18 Development and Maintenance of Configurations
  - H19 Vertical Product Procedures
  - H20 Record Retention Policy
  - H21 License Distribution Procedure
  - H22 SaaS Change Control Procedure
  - H23 Server Access Control Procedure
  - H24 Hosted Systems Support Procedure

- De software is ontwikkeld en wordt beheerd en onderhouden volgens de Software Development Life Cycle (SDLC). De oplossing wordt ontwikkeld volgens standaard processen die o.a. gedocumenteerd zijn in de interne Development Guidelines en in het ISO/IEC 27001:2013 gecertificeerde Information Security Management System van de leverancier. Wijzigingen in de code worden peer-reviewed en uitvoerig getest en gevalideerd door ons voordat een nieuwe versie van de oplossing vrijgegeven wordt en beschikbaar wordt gesteld aan klanten.
- Ter borging van de kwaliteit van onze producten en services is er een kwaliteitsmanagementsysteem (QM) ingevoerd dat voldoet aan de eisen van de nationale en internationale kwaliteitsnorm, ISO 9001. De directie controleert voortdurend de doeltreffendheid van het systeem en streeft naar voortdurende verbetering ervan.
- All of our devs are followed in a project management system with clear steps. We also use Quality Control before releasing.
- Met het platform streven wij er naar klanten zoveel mogelijk te ontzorgen. Daarom hebben we het begrip 'Compliance by Design' geïntroduceerd. Dit wil zeggen dat we ervoor zorgen dat het platform en de dienstverlening standaard compliant is en meegroeit met de relevante set van overheid brede bepalingen, kwaliteitsnormen en wet- en regelgeving op het gebied van overheidsdienstverlening (zoals BIO, AVG, WCAG, Open Standaarden forum standaardisatie en de Archiefwet).
- Het begrip 'Compliance by design' komt op verschillende manieren tot uiting in het platform en de bijbehorende dienstverlening. Het is ingebed in het platform, de onderliggende dienstverleningsprocessen en de teamcultuur. Daarnaast krijgt het aandacht bij het samenstellen van de teams en bij opleidingen en kennisborging. Hierdoor kan de focus van de samenwerking met klanten vooral gericht zijn op optimale ondersteuning van de primaire processen.
- Voor het bewaken en borgen van de software kwaliteit vormt de ISO/IE 25010-norm een belangrijke rol. Bij de invulling van deze kwaliteitskenmerken komen de hiervoor genoemde bepalingen, kwaliteitsnormen en wet- en regelgeving ook weer terug.
- Wij streven naar een cultuur waarin continue sprake is van verbetering van het kwaliteitsniveau. Dit doen we door het toepassen van:
  - De principes achter compliance -, security - en privacy by design bij de ontwikkeling en het beheer van onze oplossing.
  - Objectieve geautomatiseerde kwaliteitsmetingen van de software als integraal onderdeel van het werkproces.
  - Een continue verbeterproces en gerichte verbeteracties .
  - Een cultuur van continue verbetering binnen de teams.

18. *Indien er koppelingen worden gelegd met andere componenten, dan koppelen we bij voorkeur via REST/JSON webservices. Enerzijds om te koppelen met REST services van andere componenten, anderzijds om zelf REST services te bieden waarop andere componenten kunnen koppelen. In hoeverre ondersteunt uw oplossing in algemene zin deze technische vorm van connectiviteit?*

#### Samenvatting:

De oplossingen van alle leveranciers kunnen koppelen met REST/JSON webservices.

#### Beantwoording:

- Niet alle componenten die binnen het lab worden ingezet hanteren webservices maar zijn veelal vendor specifiek.
- Het systeem gebruikt de zeer breed geaccepteerde CURL bibliotheek om webservices te consumeren. Verder is het uitermate simpel om zelf webservices te definiëren en te publiceren.
- Onder meer de uitwisseling o.b.v. (JSON/) XML waarbij de specificaties(format e.d.) nader dient te worden gespecificeerd
- Het zaaksysteem is standaard in staat te koppelen middels web services als REST/JSON en SOAP/XML. Alle activiteiten ondersteund door het zaaksysteem kunnen, als (de afwezigheid van) gebruikersinteractie dat toestaat, ook middels deze protocollen ontsloten worden naar andere systemen. Verder sluit het platform zoveel mogelijk aan op (technische) marktstandaarden, zoals CMIS, OAuth en LDAP en de in de Nederlandse overheid gangbare open standaarden van Forum Standaardisatie.

*19. De NVWA heeft een eigen monsteradministratie. Uitgangspunt is dat alle monsters daarin worden vastgelegd. In hoeverre is het met uw oplossing mogelijk om monstergegevens uit een externe monsteradministratie te betrekken, bij voorkeur op de manier zoals beschreven onder punt 6, en bij voorkeur zonder de gegevens verplicht te moeten repliceren naar de (database van de) oplossing zelf?*

#### Samenvatting:

Alle leveranciers geven aan dat ze met hun oplossing monstergegevens uit een externe monsteradministratie kunnen betrekken. De mogelijke manieren worden hieronder beschreven.

#### Beantwoording:

- De oplossing kan met query, gegevens overnemen uit andere systemen.
- De LIMS wordt vaak gebruikt om te communiceren met bijvoorbeeld laboratoriuminstrumenten of andere business-systemen. Met ondersteuning van alle populaire uitwisselingsprotocollen is het zeker mogelijk om monstergegevens uit een externe monsteradministratie te betrekken. Dit is mogelijk door toepassing van bijvoorbeeld referenties zonder data daadwerkelijk te dupliceren naar LIMS. Chain of Custody kan gewaarborgd blijven binnen LIMS of middels communicatie naar het externe systeem.
- We bieden een compleet framework voor (geautomatiseerde) gegevensuitwisseling en zeer uitgebreide koppelingsmogelijkheden met andere systemen.
- Deze communicatie kan worden opgezet met onze standaard web-API. Deze web-API is onderdeel van onze standaardoplossing en zorgt voor een gevalideerde uitwisseling van gegevens.

- We beschikken over de volgende standaard componenten:  
 web-API - Set of web functies that can be used to exchange data  
 Service process (database) – Service application that runs task based on events or time schedule.  
 Agent (internet) – Windows application connected with the solution to automate tasks. Daarnaast beschikt de oplossing over de volgende standaardfuncties:
  - External Record – Mechanism to define that a record is owned by an external system.
  - Mapping System – Manage names of entities as they are named in other systems for translations
  - Task runner – Background task that can import data from WebResources, FTP and/or File System.
  - XML – Data import and export.
- We can create and populate fields with external URL pointing to other systems. More generally, you will have to think which system does what because you will have duplicate information.
- Referentie vanuit onze zaaksystemen naar en uitlezen van bronregistraties en -administraties, zoals de administratie voor monsters, is gebruikelijke praktijk. Een dergelijke referentie vereist in het zaakstelsel uiteraard wel opslag van een kopie van een sleutelgegeven, zoals monster-id. Zolang de toegangssnelheid van de gegevens in de bronadministratie voor deze monsters hoog genoeg is, is het kopiëren van de rest van de monstergegevens in de administratie van het zaakstelsel niet nodig. Hetzelfde sleutelgegeven zorgt ervoor dat de Chain of Custody samenhangend traceerbaar blijft over de verschillende administraties.

20. De NVWA voert een centraal DMS in dat een REST API aanbiedt volgens de CMIS standaard. Kent uw oplossing de mogelijkheid om via CMIS documenten op te slaan in en op te vragen uit een extern DMS?

Samenvatting:

Twee leveranciers ondersteunen al CMIS en kunnen documenten opvragen uit een extern DMS. Drie andere leveranciers geven aan dat het er nu nog niet is, maar wel gerealiseerd kan worden.

Beantwoording:

- Vanuit onze huidige klantbestand speelt de integratie van een DMS niet. Wel worden beelden die zijn gedigitaliseerd gekoppeld aan het onderzoek. Kortom zouden we op identieke wijze de DMS integratie kunnen doen en via Thumbnails de koppeling kunnen leggen naar het document. Het koppelen, overhalen of juist navigeren naar opslaglocaties is mogelijk. Dit kan handmatig of met applicatielogica worden gerealiseerd.
- REST wordt ondersteund waarmee CMIS documenten opgeslagen kunnen worden of opgevraagd kunnen worden. Specifieke configuratie noodzakelijk voor de koppeling.
- Dit is zeer goed mogelijk. Een compleet framework voor (geautomatiseerde) gegevensuitwisseling en zeer uitgebreide

koppelingsmogelijkheden met andere systemen wordt geboden. De gevraagde koppeling is niet standaard aanwezig, maar kan op basis van een functioneel ontwerp worden gerealiseerd.

- webservices o.b.v. (REST) API 's om documenten vanuit een extern DMS op te vragen wordt ondersteund.
- We have several connectors to DMS solutions. For instance, there is a cmis connector to Alfresco. Het gebruik van Alfresco wordt ook door een andere leverancier genoemd.
- Ja, het platform ondersteunt CMIS om documenten uit te kunnen wisselen met een extern DMS. Dit maakt het gebruik van verschillende implementaties van een extern DMS mogelijk.

*21. De NVWA heeft een centraal register organismen, ontsloten via REST services. Ondersteunt uw oplossing de mogelijkheid om basisgegevens m.b.t. organismen uit een extern register te betrekken?*

Samenvatting:

Alle leveranciers geven aan dat de oplossing die ze bieden deze mogelijkheid heeft.

Beantwoording:

- Ja, dit is mogelijk, wij zouden een (bv HL7) koppeling kunnen ontwikkelen waarmee de gegevens geautomatiseerd worden gesynchroniseerd van het externe systeem naar de LIMS
- We bieden een compleet framework voor (geautomatiseerde) gegevensuitwisseling en zeer uitgebreide koppelingsmogelijkheden met andere systemen. De gevraagde koppeling is niet standaard aanwezig, maar kan op basis van een Functioneel Ontwerp worden gerealiseerd.

*22. De NVWA werkt met specialistische meetapparatuur (zie bijlage 2: specialistische meetapparatuur). Op welke wijze kan uw oplossing koppelen met dergelijke meetapparatuur en welke standaardkoppelingen biedt uw oplossing hiervoor?*

Samenvatting:

Alle leveranciers geven aan te kunnen koppelen met dergelijk meetapparatuur. Het gebruik van xml en csv wordt door meerdere leveranciers genoemd.

Beantwoording:

- Er is ruime ervaring met het ontwikkelen van koppelingen van het LIMS met laboratoriuminstrumenten die worden toegepast in de pathologie. Daarbij wordt vaak gebruik gemaakt van HL7 koppelingen. Ons uitgangspunt is dat we elke koppeling die de opdrachtgever wenst, ondersteunen. Dit hangt uiteraard wel af van de mate waarin een koppeling met het betreffende systeem kan worden opgezet c.q. of de leverancier van dat systeem een koppeling ondersteunt.
- De LIMS wordt vaak gebruikt om te communiceren met bijvoorbeeld laboratoriuminstrumenten, Process Information Management Systems /

- Manufacturing Execution Systems (PIMS / MES) en ERP / SAP. Alle populaire gegevensuitwisselingsformaten worden ondersteund, waaronder CSV, XML, Webservices, directe databasetoegang (SQL/ ODBC/ JDBC), API's, externe functieaanroepen (RFC's), OLE Automation, OLE for Process Control (OPC), ActiveX, FTP, TCP/IP Sockets, e-mailberichten (SMTP/ MAPI/ VIM), RS-232 seriële communicatie, ASTM/HL7 protocollen, etc.
- We bieden een compleet framework voor (geautomatiseerde) gegevensuitwisseling en zeer uitgebreide koppelingsmogelijkheden met specialistische meetapparatuur.
  - Er kan bi-directioneel informatie uitgewisseld worden met de bij de NVWA in gebruik zijnde laboratorium instrumenten o.b.v. verschillende interfacetechnieken (o.a. ESB, Web Services, webAPI, file exchange ) en ondersteunt event driven integratie. Het platform biedt een gestandaardiseerde generieke interface voor instrumentkoppelingen op basis van CSV en kan ook aansluiten op reeds aanwezige koppelingsplatformen.
  - De Open Interface bestaat uit de volgende standaard Componenten:
    - Web-API - Set webfuncties die kunnen worden gebruikt om gegevens uit te wisselen.
    - Serviceproces (database) - Diensttoepassing die taak verricht op basis van gebeurtenissen of tijdschema.
    - Agent (internet) - Windows applicatie verbonden met de LIMS om taken te automatiseren.
  - Standaard functies:
    - Extern record - mechanisme om vast te stellen dat een record eigendom is van een extern systeem.
    - Mapping System - Beheer namen van entiteiten zoals ze worden genoemd in andere systemen voor vertalingen.
    - Taskrunner - Achtergrondtaak die gegevens kan importeren vanuit WebResources, FTP en / of File System.
    - XML - Data import en export.
  - De interfacing van instrumenten via serial, USB or TCP-IP connecties aangevuld met additionele, configureerbare interfacing voor hoog geautomatiseerde doeleinden o.b.v. Direct network connection of Database links.
  - De hardwareinterfacing van analyseapparatuur zonder eigen software met Native Subsystem Integration voor verwerking en interpretatie van meetwaarden, berekening van resultaten, weergave limietoverschrijdingen en QC verzoeken etc.
  - We provide an EDI module. This module allows to retrieve datas from instruments. You have to export data from the instrument in a structured format (csv, xls, txt,...) and "send" it to the solution by email or by saving to a specific location. This module allows you to program yourself on a white screen. This module allows to reduce the costs of the connections with the instruments.
  - Dankzij het integratiecomponent biedt het platform de mogelijkheid de benodigde interfaces voor de specialistische meetapparatuur, maar ook de

applicaties in het NVWA Componenten landschap, op eenvoudige wijze te configureren en integreren. De sector-overschrijdende expertise binnen zowel de overheid, laboratoriumwereld als de fabrikanten van meetinstrumenten die wij hebben, zorgt ervoor dat alle meet- en andere systemen met elkaar worden verbonden op basis van de nieuwste configuraties, uitbreidingen en binnen de overheid verplichte standaarden. Het platform bevat op dit moment geen voor-geconfigureerde interfaces voor meetapparatuur, maar biedt door configuratie de mogelijkheid om de benodigde uitbreidingen op korte termijn en op de best mogelijke wijze te realiseren. De oplossing ondersteunt wel alle binnen de overheid verplichte standaarden en protocollen die nodig zijn voor betrouwbaar berichtenverkeer. De structuur van de software maakt elke uitbreiding mogelijk. Op zodanige wijze dat:

- Koppelingen compliant zijn aan de overheidsrichtlijnen.
- Analysegegevens op een gestructureerde wijze worden toe- en samengevoegd in talrijke formaten (zoals XLS, XML, CSV).
- De workflow voor de ondersteuning van de LIMS-processen op basis van de specifiek behoefte van het NRC kan worden geoptimaliseerd.
- Door vergaande digitalisering, handmatige invoer tot een minimum wordt beperkt om fouten te voorkomen.

*23. Op welke wijze worden gegevens technisch opgeslagen in uw oplossing en welke standaard databasemanagementsystemen ondersteunt u?*

Beantwoording:

- Alle data wordt vastgelegd in een relationele MS SQL database. Het gebruik van deze database wordt door meerdere leveranciers genoemd. De LIMS voorziet daarbij in een tabellenstructuur waarin aangemaakte velden voor de vast te leggen gegevens van overige bronnen en kan conform de gegevenstype invulling geven aan technische parameters.
- Alle gegevens worden in principe in onze database opgeslagen. Met uitzondering van bestanden welke mogelijk in een andere database van ons kunnen worden opgeslagen of met een verwijzing naar een externe opslag.
- Meerdere leveranciers geven aan dat verschillende DBMS-en worden ondersteund.
- Uitgangspunt hierin is dat u als klant het platform bepaalt. In de praktijk zijn MS SQL Server en Oracle het meest voorkomend, waarbij we steeds vaker vanuit de Belgische overheid PostgreSQL gevraagd zien en toepassen. MS SQL Server en Oracle worden genoemd door meerdere leveranciers.
- Een Microsoft SQL Server wordt gebruikt als een databaseserver met de primaire functie van het opslaan en ophalen van gegevens. De Microsoft SQL Server is een databasebeheersysteem (DBMS) dat is ontworpen om, onder andere, databases te definiëren, samen te stellen en te doorzoeken om gegevensbewerkingen uit te voeren zoals toevoegen, bewerken, verwijderen enz. Functies van SQL Server omvatten de ondersteuning van

indexering en LINQ, verbeterde beveiliging, eenvoudige toegang en de verwerking van vele records tegelijkertijd.

- Bestanden van verschillende gegevenstypen worden centraal opgeslagen in het platform. Gegevens worden opgeslagen als elektronische records in de database, maar worden opgehaald en gevisualiseerd in het oorspronkelijke formaat.
- Voor koppeling met DMBS'en voor externe administraties, ook van andere leveranciers, zijn verschillende technieken beschikbaar.
- Formaat van interne opslag van de gegevens van een zaak is standaard in de vorm van een aggregaat (in een CLOB-attribuut). Een aggregaat is een xml-bericht dat het gehele of een deel van het zaakprofiel bevat. Dit bericht kan ook opgeslagen worden in een NOSQL-DBMS als MongoDB.
- Zonder verder op de diepere achtergrond in te gaan, biedt het opslaan van een aggregaat verschillende technische voordelen die voornamelijk de aanpasbaarheid van het zaksysteem ten goede komt. Meestal kopieert de applicatie daarnaast ook een deel van de gegevens naar een relationele database voor koppeling met de BI- of verantwoordingscomponent.
- Als directe toegankelijkheid door andere systemen op de aggregaatopslag vereist is, bestaat de optie om gestructureerd, relationeel op te slaan. Die keuze maken we in overleg met de opdrachtgever. We raden aan om die keuze bij voorbaat al te maken voor administraties die ook na afronding van het onderzoeksproces waar ze uit voortkomen nog moeten kunnen worden geraadpleegd.
- Voor generieke technische koppeling met relationele databases hebben wij de keuze uit ons-ORM (Object Relation Manager) of ORDS (specifiek voor Oracle, eerder toegepast bij de NVWA).

#### **1.4 Informatiebeveiliging en privacy**

24. *Kunt u uw beleid rondom informatiebeveiliging en privacy in grote lijnen schetsen?*

Beantwoording:

- Alle data wordt ondergebracht in een systeem dat zich bevindt op de fysieke klantlocatie. De leverancier gaat er vanuit dat de opdrachtgever zorgdraagt voor een (adequaat beveiligde) ICT-infrastructuur. Deze ICT-infrastructuur wordt verondersteld te voldoen aan door de leverancier gestelde systeemvereisten.
- De opdrachtgever is verantwoordelijk voor het opstellen van een adequaat back-upbeleid, het uitvoeren van de back-up's en het testen van de adequate werking van de back-up. De leverancier adviseert de opdrachtgever hierin.
- Partijen sluiten een Verwerkersovereenkomst af. De leverancier is geen verwerker in de context van de werkprocessen van de opdrachtgever maar wel bij het uitvoeren van onderhoudswerkzaamheden en het verhelpen van eventuele problemen.

- Voor het uitvoeren van onderhoudswerkzaamheden en het verhelpen van eventuele storingen is het nodig dat de leverancier toegang krijgt tot de systemen van de opdrachtgever. De toegang tot de systemen van de klant is vanuit de leverancier strikt gereguleerd; door middel van een autorisatiematrix mogen alleen die medewerkers toegang verschaffen tot de systemen indien zij werkelijk voor hun werkzaamheden deze toegang nodig hebben. Medewerkers moeten een geheimhoudingsverklaring ondertekenen als onderdeel van de arbeidsovereenkomst met de leverancier. Periodiek wordt er voor de medewerkers van de leverancier een Verklaring Omtrent Gedrag opgevraagd.
- Zowel het verlenen van de autorisaties (organisatorisch) als de technische toegang (beschikt de medewerker over de middelen zich toegang tot het systeem van de opdrachtgever te verschaffen?) Wordt periodiek onderworpen aan interne audits.
- Het softwareontwikkelproces van de leverancier is opgezet op basis van een Beleid voor beveiligd ontwikkelen. Informatiebeveiliging en aandacht voor potentiële risico's is structureel onderdeel van de verschillende stappen in het softwareontwikkelproces.
- De omvang van de inspanning kan verschillen maar bij elke wijziging en bij elk project wordt er door de leverancier een risicobeoordeling gedaan. De uitkomst van deze risicobeoordeling bepaalt mede of er, naast algemene maatregelen zoals hierboven beschreven, aanvullende of specifieke maatregelen noodzakelijk zijn. Voor zover deze relevant zijn voor de opdrachtgever worden de resultaten van een risicobeoordeling met de opdrachtgever gedeeld. Risicobeoordelingen worden ook samen met de opdrachtgever uitgevoerd.
- In alle gevallen waarin sprake is van planbare werkzaamheden, zoals nieuwe systeemimplementaties, het uitvoeren van belangrijke upgrades of ander onderhoud aan de systemen, worden werkzaamheden projectmatig en planmatig uitgevoerd. Er vindt altijd afstemming plaats met de opdrachtgever zodat duidelijk is welke impact de geplande werkzaamheden hebben op de productiesystemen en welke eventuele maatregelen daarvoor genomen moeten worden.
- Het toepassen van het OTAP-principe beschouwt de leverancier als een standaard aanpak.
- Een leverancier verwijst naar zijn Information Security Management System policy.
- De leverancier kenmerkt zich door een hoge mate van bewustzijn op het vlak van privacy en security. Onder verantwoording van de afdeling Quality Assurance (QA) worden de laatste ontwikkelingen op het gebied van privacy en security actief opgevolgd. Daarbij hanteert de leverancier een open communicatie met haar klanten over relevante veranderingen in haar beleidsmaatregelen.
- Waarborgt de veiligheid van alle informatie en heeft hiertoe technische en organisatorische maatregelen genomen welke onderdeel vormen van het Service Level Agreement (SLA)
- Twee leveranciers geven aan zich te conformeren aan de Europese richtlijnen General Data Protection Regulation (GDPR)

- Het is voor de LIMS van groot belang dat de gegevens die hierin verwerkt worden veilig worden verwerkt en opgeslagen. De NVWA maakt in dit kader gebruik van mensen, processen, middelen. Als wij de regeling beheren en exploiteren voor de NVWA worden wij deel van de verwerkingsketen van de NVWA. Het is daarom van groot belang dat de informatiebeveiliging rond het LIMS en de dienstverlening op orde is. Informatiebeveiliging, bedrijfscontinuïteit, cyber-weerbaarheid en privacy maken integraal deel van onze dienstverlening. De scope van ons informatiebeveiligingsbeleid omvat zowel de organisatorische onderdelen die activiteiten verrichten voor het LIMS als de bedrijfsmiddelen (in de breedste zin van het woord, zoals IT-systemen, platformen, applicaties, documenten, apparaten, faciliteiten, mensen, gedachtengoed, enz.) die gebruikt worden voor de opslag, verwerking en het transporteren van informatie van de LIMS-applicatie. Om informatiebeveiliging effectief binnen de organisatie te borgen passen we een Plan-Do-Check-Act (PDCA) cyclus toe waarbinnen stelselmatig en continu aan verbetering wordt gewerkt. Het beleid biedt de kaders waarbinnen bewogen wordt. Deze cyclus wordt over de gehele organisatie uitgevoerd als onderdeel van de reguliere bedrijfsvoering. De PDCA cyclus is een jaarlijks proces, hetgeen ervoor zorgt dat er minimaal jaarlijks bijgestuurd kan worden op basis van de uitkomsten van risico analyses, bevindingen, dreigingen, etc.
  - Hiernaast passen wij binnen onze dienstverlening en oplossing het principe van 'compliance by design' toe zoals uitgebreid beschreven bij vraag 17.
- a. *Licht toe hoe u specifieke risico's met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid van de mogelijk te aanbesteden opdracht vertaalt naar concrete maatregelen in uw dienstverlening.*

**Samenvatting:**

De rol van de medewerkers met betrekking tot vertrouwelijkheid en geheimhouding wordt door meerdere leveranciers genoemd.

**Beantwoording:**

- Er zijn standaard procedures rondom de genoemde topics. Voor risico's t.a.v. beschikbaarheid van het systeem zijn diverse mogelijke oplossingen om dit te voorkomen. Afhankelijk van de deployment strategie worden specifieke acties uitgezet. Denk hierbij aan Infra/Cloud Redundant Deployment, Fail-over systems, High Availability modus. Integriteit van data kan o.a. worden gerealiseerd en beveiligd middels database encryptie. De audit trail en het GxP (stelsel van kwaliteitssystemen ) compliancy middelen ondersteunen hierin. We bieden ingebouwde beveiligingen voor vertrouwelijkheid van data. Specifieke oplossingen worden ten tijde project uitgewerkt door bijvoorbeeld diverse rollen en levels van beveiliging te definiëren. Met betrekking tot dienstverlening is de oplossing GDPR compliant.
- We monitoren ook de applicatie. Hier kan ook een dashboard voor worden ingericht. Hoe dit eruit moet zien, stemmen we met de klant af. Mocht er

toch een keer een hapering zijn, dan kunnen we dit ook op afstand via een remote desktop herstellen.

- Het Information Security Management System is gecertificeerd volgens ISO/IEC 27001:2013, dat beschrijft hoe procesmatig met het beveiligen van informatie om te gaan, met als doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie zeker te stellen. Risico's met betrekking tot beschikbaarheid, integriteit en vertrouwelijkheid zijn geïdentificeerd, gedocumenteerd en behandeld.
- Het managementteam zorgt ervoor dat het informatiebeveiligingsbeleid en de informatiebeveiligingsdoelstellingen worden vastgesteld en verenigbaar zijn met de strategische richting van de organisatie. Daarnaast beoordeelt het managementteam het ISMS elk kwartaal om de blijvende geschiktheid, toereikendheid en effectiviteit ervan te waarborgen. Middelen die nodig zijn voor het opzetten, implementeren, onderhouden en continu verbeteren van het ISMS worden beschikbaar gesteld.
- Medewerkers zijn door het management verplicht om informatiebeveiliging toe te passen in overeenstemming met het vastgestelde beleid en de vastgestelde procedures en hebben de juiste bewustwordingstrainingen en -trainingen en regelmatige updates van het beleid en de procedures ontvangen, voor zover relevant voor hun functie. Een andere leverancier geeft aan dat een contractuele verplichting van medewerkers is om vertrouwelijk om te gaan met klantgegevens en de rol van de medewerker wordt ook benadrukt door een andere partij.
- Interne audits worden uitgevoerd om te bepalen of procedures, controles, processen, regelingen en andere activiteiten binnen het ISMS in overeenstemming zijn met de ISO 27001-normen, de toepasselijke regelgeving en de interne documentatie van de organisatie, of ze effectief geïmplementeerd en onderhouden worden en of ze voldoen aan de beleidsvereisten en de 11 gestelde doelen. Er wordt een jaarlijks intern auditprogramma opgesteld en goedgekeurd door het management, en elk kwartaal worden interne audits uitgevoerd. Auditbevindingen (nonconformities of observaties) worden ingevoerd in het issue tracker en support systeem en worden toegewezen, opgelost en gemonitord.
- Leverancier is bereid om een Non-Disclosure Agreement (NDA) te ondertekenen ten aanzien van de beschikbaarheid, integriteit en vertrouwelijkheid van alle beschikbaar gesteld informatie.
- We define specific measures with our customers.
- Door de flexibiliteit van het platform worden processen gemodelleerd conform de eisen en wensen van de NVWA (Functional Fit). Deze flexibiliteit zit hem niet alleen in processen, maar ook in de infrastructuur. Op basis van de non-functionals wordt de infrastructuur achter het platform geschaald. Gemaakte afspraken leggen wij vast in het ontwerp van de omgeving en in de Service Level Agreement (SLA) en Dossier afspraken en procedures (DAP). Deze afspraken worden gemonitord en hierover wordt periodiek gerapporteerd. Een andere leverancier geeft ook dat geheimhouding en beschikbaarheid terugkomt in de SLA. Deze zelfde methodiek wordt toegepast voor de integriteit van vertrouwelijkheid van

de gegevens. Op basis van de Privacy Impact Assessment (PIA) wordt de dataclassificatie vastgesteld en worden de infrastructuur en de processen daaromheen vastgesteld. Afspraken leggen wij onder andere vast in het informatiebeveiligingsplan.

Voorbeelden van enkele concrete maatregelen:

- Reguliere audit door een security officer.
- Dubbel uitvoeren van infrastructuur componenten.
- Periodieke penetratietesten.
- Jaarlijkse toetsing van onze medewerkers op onze "code of ethics".

- b. Licht toe hoe u in uw beleid op de hoogte blijft van nieuwe risico's die bekend worden (denk aan responsible disclosure, zero day exploits, waarschuwing vanuit NCSC en/of leveranciers).*

Beantwoording:

- Op dagelijkse basis worden websites geraadpleegd waar informatie met betrekking tot dit soort risico's te vinden is. Actuele ontwikkelingen worden gemonitord en indien noodzakelijk worden bijvoorbeeld patches direct uitgerold in de ICT-infrastructuur.
- De hosting partner past de nieuwste technologie toe om de systemen te beveiligen. Een onderdeel hiervan is een proactieve alarmering vanuit het security operations center (SOC) ondersteund door de leveranciers van de security componenten. Een andere leverancier geeft aan ook aan dat security management in de hostingdiensten geïntegreerd zijn.
- Dit is geïmplementeerd en gedocumenteerd en wordt beheerd in het ISO/IEC 27001:2013 gecertificeerde Information Security Management System.
- Mede op basis van deelname relevante usergroups, partner van diverse technologieleveranciers en pro-actieve research risico-analyse worden acties genomen zoals het beschikbaar stellen van test/patches of workarounds voor gebruikers van de oplossing.
- Er is een Security Operation Center (SOC) waar vanuit verschillende klanten bediend worden. Het SOC ontvangt pro-actief alle meldingen vanuit het NCSC en vertaalt deze naar potentiële acties voor klanten van het SOC. Bij cruciale melding wordt er direct contact opgenomen met de klanten om (herstel)acties in te plannen. Naast meldingen vanuit het SOC zijn vulnerabilities scans standaard onderdeel van de dienstverlening. Periodiek worden alle software componenten gecontroleerd op updates en bekende risico's. Bij noodzakelijke updates wordt er een voorstel gedaan voor het doorvoeren van de updates. Iedere nieuwe major en minor release wordt gecheckt middels de OWASP dependency checker.

c. *Kunt u schetsen hoe uw incident en response management is ingericht?*

Samenvatting:

Alle leveranciers hebben het incident en response management prices vastgelegd in een document, zodat alle medewerkers en klanten weten hoe dit afgehandeld dient te worden. Het merendeel van de partijen geeft aan dat dit proces beschreven is in de SLA.

Beantwoording:

- Conform de certificering voor ISO 27001 en NEN7510 is er een proces voor incidentbeheer ingericht. Daarmee weten betrokkenen welke situaties als incident gemeld moeten worden, op welke wijze zij dit moeten doen en is duidelijk wie er verantwoordelijk is voor de behandeling c.q. afhandeling van de meldingen. Meldingen worden geregistreerd en de behandeling wordt gedocumenteerd. Jaarlijks worden de meldingen en de afhandeling geëvalueerd. Deze evaluatie wordt ook meegenomen in managementrapportages.
- De systemen worden 24/7 gemonitord vanuit het netwerk operation center van de hosting partner. Tickets die hieruit voortkomen worden na triage geëscaleerd naar het security operation center of naar ons. Na prioritisering worden de tickets volgens de SLA afgehandeld. Tickets worden vastgelegd in een centraal ticket systeem en zijn inzichtelijk binnen de organisatie waar deze worden gegenereerd.
- Het incident en response management is beschreven als onderdeel van het Quality Management en beschrijft de afhandeling van de binnenkomende call bij de Help Desk. Ondersteuning gebeurt rechtstreeks per telefoon, e-mail of fax. Als de call niet direct kan worden afgesloten volgt een escalatie van de call en informeert de verantwoordelijke medewerker de klant over de activiteiten die nodig zijn.
- We are using monitoring tools and we receive updates and alerts. For incident we use Jira system.
- Incidenten kunnen zowel door u als klant, door de System Integrator (SI) of door de 24\*7 van de SI aangemeld worden. Aanmelden van incidenten richting onze skilled helpdesk kan zowel telefonisch als via mail. Wij onderscheiden 4 type incidenten (Zeer hoog, Hoog, Middel en Laag). Definities van deze type komen wij gezamenlijk overeen in de DAP evenals de oplostijden. Alle incidenten worden door onze servicedesk geregistreerd en hierover wordt periodiek gerapporteerd. Voor incidenten van type Zeer Hoog wordt direct een incident manager en een oplosteam aangesteld. De incident manager is verantwoordelijk voor het aansturen van het oplosteam en verzorgt de communicatie richting de NVWA. Afhankelijk van de overeengekomen afspraken wordt het incident binnen de gestelde oplostijden opgelost. Mocht dit niet haalbaar blijken, informeert de incident manager de NVWA hierover en communiceert de verwachte doorlooptijden. Na afronding van het incident wordt een Root Cause Analyse (RCA) opgesteld en gedeeld met de klant. Onderdeel van deze RCA is verbeterpunten ter voorkoming van herhaling van hetzelfde incident.

*25. Geef aan of u gecertificeerd bent voor: ISO 27001, voldoet aan ISO 27017 en/of ISO 27018. En licht toe, hoe stelt u ons in staat dat wij kunnen vaststellen dat u aan genoemde ISO normen voldoet?*

Samenvatting:

Het merendeel van de leveranciers is ISO27001 gecertificeerd, op twee leveranciers na. Als bewijs kunnen de gecertificeerde leveranciers een certificaat overhandigen.

Beantwoording:

- Het managementsysteem is gecertificeerd voor ISO27001 en NEN7510. We zijn geen Cloud Service Provider en niet gecertificeerd voor ISO 27017 en/of ISO 27018. Daarnaast is het mogelijk om in overleg een audit uit te voeren. Periodieke audits met leveranciers doen we zelf.
- Onze hosting partner is ISO27001 en SSAE 16 SOC-2 gecertificeerd. We voldoen (niet gecertificeerd) aan ISO27001:2013 en heeft een verklaring van toepasbaarheid, risicobeoordelingen en IT Security Management Procedures en beleid. Dit staat beschreven in ons Kwaliteitshandboek dat is getoetst aan ISO9001:2015 en waar we tegen gecertificeerd zijn.
- Het Information Security Management System is gecertificeerd volgens ISO/IEC 27001:2013.
- Als het wordt aangeboden als SAAS wordt gebruik gemaakt van een Europees Datacenter in bezit van een tier 3/ tier 4 classificatie en ISO 27001 (ISO 17021 en ISO 27006) gecertificeerd en werkend volgens de praktijken in overeenstemming met ISO NEN 27002.
- We zijn ISO 27001 gecertificeerd. Desgewenst kan de NVWA een externe audit uit laten voeren op onze processen.

*26. Verwachte beschikbaarheid tijdens kantoortijd is tussen 7:00 - 19:00 uur (Nederlandse tijd). In geval van crisissituaties heeft de oplossing heeft een hoge beschikbaarheid nodig van 6:00 - 22:00 uur, met mogelijkheden voor directe opschaling ook in het weekend. Kunt u dit leveren en hoe snel kunt u opschalen?*

Samenvatting:

Alle leveranciers geven aan de mogelijkheid te hebben om af te wijken van de standaard kantoortijden. Deze afwijkingen worden bij het merendeel vastgelegd in de SLA.

Beantwoording:

- Deze vraag wordt geïnterpreteerd als de beschikbaarheid van de Servicedesk. Alvorens hier op in te gaan een korte opmerking over het systeem zelf. Het systeem opereert in de ICT-infrastructuur van de opdrachtgever en is in beginsel 24/7 beschikbaar. Een andere leverancier geeft ook aan dat het systeem altijd beschikbaar is behalve tijdens de onderhouds- en update momenten die in samenspraak met de klant kunnen worden ingepland.
- Onze ervaring leert dat, indien het systeem opereert in een ICT omgeving die voldoet aan de door ons gestelde systeemvereisten, de

beschikbaarheid zeer hoog is (meer dan 99%). De afgelopen jaren is bewezen dat er geen calamiteiten zijn ontstaan bij het gebruik van onze software. We hebben een bewezen methodiek gevonden die met vertrouwen updates en upgrades mogelijk maakt. Beschikbaarheid van de servicedesk, de afgesloten exploitatieovereenkomst en dienstbeschrijving voorziet standaard in openingstijden tussen 08:30 – 17:00 uur. Daarin kunnen we in geval van de NVWA afwijken en ruimere openingstijden hanteren. De overeenkomst voorziet in een Governance procedure waarmee te allen tijde duidelijk is wie met wie communiceert in een (crisis) situatie. Afhankelijk van de situatie kan er geschakeld worden met onze CTO/COO of zelfs CEO.

- In het geval van calamiteiten waarvan de oorzaak feitelijk buiten de software van ons ligt, zoals langdurige server issues, brand, etc zullen we altijd het maximale doen om met inzet van onze specialisten een tijdelijke of definitieve oplossing te vinden.
- De afspraken met opdrachtgever worden vastgelegd in de SLA en elk kwartaal geëvalueerd. Op basis van de evaluatie worden eventueel afspraken bijgesteld. De servicemanager is hiervoor verantwoordelijk.
- Een uptime van de Cloudservices van 99,9% wordt gegarandeerd. Voor de applicatie zal de uptime variëren vanwege de upgrades/onderhoudsmomenten.
- Hotline en klantenservice tijdens de kantoortijden van maandag tot en met vrijdag (07.00 -17.00). Mogelijkheden om hiervan af te wijken of opschaling kunnen worden overeengekomen en zullen vervolgens onderdeel zijn van het SLA.
- It can be done through specific contracts. Support is also available 20 hours a day. We already have that kind of contract with some customers and they never had to use it. The solution is reliable. The major risk is the infrastructuur.
- Dit kan geleverd worden, we beschikken standaard over een 24/7 service organisatie. Op basis van de overeengekomen SLA kunnen we binnen enkele uren opschalen naar het gewenste niveau.

*27. Kunt u schetsen hoe de backup en recovery is georganiseerd en kunt u aangeven wat de maximale 'time to recovery' is?*

Beantwoording:

- De opdrachtgever is verantwoordelijk voor het beschikbaar stellen van een geschikte managed ICT-infrastructuur. Onderdeel daarvan is ook dat de opdrachtgever zelf verantwoordelijk is voor het opstellen van een adequaat back-upbeleid, het uitvoeren van de back-up's en het testen daarvan. We adviseren de opdrachtgever met betrekking tot het opstellen van een back-upbeleid en de keuzes die gemaakt moeten worden met betrekking tot de verschillende componenten.
- Er wordt elk uur een incremental backup gemaakt en dagelijks een full backup ('s nachts). Er wordt een maximale recovery tijd (RTO, Recovery Time Objective) gehanteerd van 4 uur. Eventueel data verlies (RPO, Recovery Point Objective) is maximaal 1 uur. Let op dat die uit gaat van een worst-case scenario.

- Een volledige kopie van de productiedatabases van de systemen van de klant wordt elke dag gemaakt tussen 22.00u en 04.00u. Bovendien worden alle nieuwe transacties sinds de laatste volledige back-up gekopieerd in incrementele transactielogboekback-ups om de 10 of 60 minuten, afhankelijk van het bijbehorende back-upbeleid. De back-ups worden eerst lokaal opgeslagen. Tijdens het back-upproces wordt gecontroleerd of de hash van de back-up overeenkomt met die in de database. Indien correct wordt het backupproces voltooid en als succesvol beschouwd waarna de backup naar de Object Store wordt gekopieerd. Het backup proces wordt afgebroken als de hash niet correct is of niet gecontroleerd kon worden of als de backup om een andere reden niet voltooid kon worden. Als dit het geval is zal het Support Team automatisch op de hoogte worden gebracht en zal er een issue met hoge prioriteit in het issue tracker systeem worden gelogd. Een lid van het Supportteam zal dit probleem zo snel mogelijk oplossen. Alle volledige en tussentijdse back-ups worden lokaal bewaard voor een periode van 1 dag tot de volgende succesvolle volledige back-up beschikbaar is. In de Object Store worden back-ups ten minste 30 dagen bewaard. Voor clientsystemen die niet onder het High-Availability back-upcontract vallen, is er geen specifieke periodieke test voor het terugzetten van de databaseback-ups. Het proces voor het terugzetten van de back-ups zelf wordt getest tijdens de ontwikkelings-/QA-cyclus wanneer het nodig is om lokaal te debuggen of te testen met een (test-, niet-client-) database die specifieke gegevens bevat. Een vooraf geconfigureerde (gedeelte) secundaire server staat stand-by in geval van een incident met de primaire (client) server. Dit betekent dat wanneer de primaire (client) databaseserver en/of de webserver uitvalt, een (tijdelijk) systeem kan worden opgezet op een andere webserver terwijl de primaire systemen worden hersteld. Deze secundaire server is niet permanent in bedrijf, maar wordt alleen gestart wanneer een (client)systeem tijdelijk moet worden opgezet om de continuïteit van de (client)werkprocessen te waarborgen. Deze zelfde server wordt ook gebruikt voor het testen van de database restore voor klanten met een High-Availability Backup contract. Het tijdelijke systeem met een installatie van de (client) applicatie en teruggezette database zal binnen één werkdag beschikbaar zijn voor gebruik. Sommige klanten hebben een High-Availability contract. Het doel van een hoge beschikbaarheid van gegevens is het minimaliseren van gegevensverlies in het geval dat de server die de database host corrupt of down is en niet meer hersteld kan worden. Daarom wordt, als onderdeel van de High Availability services elke 10 minuten een incrementele transactionele backup gemaakt. Dit betekent dat een dataverlies van 10 minuten de maximale hoeveelheid data is die verloren kan gaan. Alle tussentijdse back-ups worden 7 dagen bewaard en er worden dagelijks volledige back-ups genomen. Om ervoor te zorgen dat de gegevens met succes zijn geback-up't, worden om de drie maanden periodieke hersteltests uitgevoerd door een lid van het Support Team. Een probleem met betrekking tot deze hersteltests, met inbegrip van alle testresultaten, moet in het Issue systeem worden geregistreerd. Zodra er een storing wordt geconstateerd in de data backup- en restore-procedures, ontvangt

het Support Team een e-mail dat er een storing is. Support zal dan direct proberen de situatie te verhelpen om de normale backup- en restore-procedures te herstellen en een hoge beschikbaarheid te garanderen.

- Beschikbaarheidscontrole en back-up zijn onderdeel van het overeen te komen SLA. We garanderen hierin een beschikbaarheid van 99,9% indien SAAS op jaarbasis.
- There is a possibility to have a back-up on another continent. We do recommend this.
- De afspraken rond Backup en Recovery zijn vastgelegd in het "Disaster Recovery and Continuity Plan". Backups bestaan uit 'VM Snapshots' waarin als het ware een 'foto' wordt genomen van de toestand van de toestand van de software op dat moment. De backups van de data in de databases worden iedere 12 uur uitgevoerd. In het platform wordt de 'time to recovery' gesteld op maximaal 36 uur na de eerste escalatie

*28. In geval van scenario 1 (SaaS) en scenario 2 (Outsourcing via System Integrator) en uw oplossing wordt ontsloten via een beveiligde internetverbinding, hoe kunt u aantonen dat u de afgesproken beschikbaarheid kunt leveren?*

Deze vraag is alleen beantwoord door de leveranciers die deze scenario's aanbieden.

Beantwoording:

- De afgesproken beschikbaarheid is opgenomen in de SLA overeenkomst. Dit wordt door nog drie leveranciers aangegeven.
- We bieden aan via Amazon Web Services (AWS) welke behoort tot meest redundante datacentre wereldwijd. Kans dat uw lokale internet uitvalt is groter dan dat AWS uitvalt.
- De oplossing als SAAS wordt vanuit het Europese Datacenter geleverd waarbij een beschikbaarheid van de applicatiesoftware op het aansluitpunt van de door Opdrachtgever beschikbaar gestelde server op het internet wordt gegarandeerd van gemiddeld 99,9% op jaarbasis.
- De verantwoordelijkheid voor een offline back-up ligt bij de Opdrachtgever.
- Indien de NVWA de oplossing afneemt op basis van scenario 1 of 2 zullen wij gebruik maken van onze service managementprocessen en maandelijks of zoveel meer als nodig een SLA-rapportage opstellen. In deze rapportage wordt ook gerapporteerd over de afgesproken beschikbaarheid.

*29. In geval van scenario 2 (Outsourcing bij een System integrator) en scenario 3 (twee kavels pakket en System Integrator) en de oplossing wordt aangeboden vanuit een datacentre, hoe hebt u Business Continuity Management (BSM) ingericht?*

Beantwoording:

- Er is hiervoor een Business Continuity Plan uitgewerkt die ter inzage via een Non Disclosure Agreement beschikbaar kan worden gesteld. Als onderdeel van de big T organisatie wordt volgens het Continuous Improvement principe continue nagedacht over bedreigingen en maatregelen die zowel preventief, detectief, repressief als correctief noodzakelijk zijn. Daarin speelt ook het IT landschap voor intern en extern gebruik en wat nauw samenhangt met informatiebeveiliging en kwaliteitsmanagement.
- Dit zal afhankelijk zijn van de gekozen hosting provider.
- Er is een Business Continuity Management beleid en strategie opgesteld als onderdeel van het ISO/IEC 27001:2013 ISO27001 gecertificeerde Information Security Management System (ISMS). Dit beleid wordt iedere 6 maanden gecheckt en bijgewerkt waar nodig. De beveiligingsregels zijn en worden periodiek getest door externe partijen. Onder meer zorgen deze regels ervoor dat toegang tot servers beperkt is tot alleen geautoriseerde gebruikers (support, maintenance). Alle toegang tot servers wordt vastgelegd. Daarnaast waarborgen deze ook de laatste security updates, zowel op het besturingssysteem, de database als de website. Updates van de server gaan via een geautomatiseerd proces, waardoor er geen toegang tot de server nodig is.
- Op dit moment geen BSM voor deze scenario's actief, maar nader te bepalen in overleg met de System Integrator.
- All scenarios are possible. Basically, you have to determine what type of SLA you want, determine the backup and restore goals, define the monitoring of the system.
- In het geval van scenario 2 zijn daar nadere afspraken over te maken, die vastgelegd worden en waarover gerapporteerd wordt. Zo kunnen er bijvoorbeeld afhankelijk van wensen en eisen zaken dubbel uitgevoerd worden (geografische spreiding). In geval van scenario 3 zien wij alleen DICTU als een realistische optie. In dat geval worden de afspraken ook rechtstreeks tussen de NVWA en DICTU gemaakt.

*30. In welke mate is in uw oplossing de betrouwbaarheid van de data geborgd te maken met vastlegging van specifieke gegevens die van belang zijn in het diagnostisch proces (denk aan de validatie, controlemechanismen, logging/monitoring ten aanzien van ISO 17025)?*

Samenvatting:

Vier leveranciers geven aan dat de gegevens worden gevalideerd op het moment van invoer.

Beantwoording:

- Er wordt de mogelijkheid geboden om invoerinstructies te tonen aan de eindgebruikers op veld- en/of paginaniveau. Daarin kunnen ook de grenswaarden worden aangegeven.
- Daarnaast geven ook meerdere leveranciers aan dat wijzigingen worden vastgelegd.

- Alle wijzigingen in het systeem worden automatisch geregistreerd als een afzonderlijke audit parameter (controlelogboek). Op alle entiteiten vinden audits plaats die veranderingen registreren. Alle audits zijn doorzoekbaar en het is mogelijk om op audit informatie selecties uit te voeren, onder andere met behulp van datalists en/of geparametriseerde rapportages. Alle audit informatie kan actief worden gebruikt in rapportages en berekeningen (statistieken). Zo worden ook fouten gelogd en kan er met behulp van de 'entity event' functionaliteit voor worden gezorgd dat er bij een bepaald type fout (trigger) een rapportage wordt samengesteld en zodra deze is gegenereerd (trigger) per e-mail wordt verzonden naar de LIMS-admin(s). Ook is het mogelijk om deze notificaties / alarmeringen te tonen op real-time dashboards in het systeem.
- Er vindt een uitgebreide logging plaats van transacties en handelingen van de gebruikers binnen het systeem, niet alleen bij initiële handelingen maar ook indien gegevens worden aangepast.
- Alle gegevens zijn vastgelegd in een backend MS SQL relationele database welke los van de applicatie inrichting volledig te back-uppen is als data. Daarin kan er ook gekozen worden voor een MS SQL farm inrichting zodoende bij een failover de data ook weer snel toegankelijk is als front end van de applicatie inrichting.
- De oplossing ondersteunt laboratorium compliancy voor ISO17025 met standaard modules voor Document Management, Training Management, Investigation Management en Uncertainty Measurement mogelijkheden.
- Integriteit van data kan o.a. worden gerealiseerd en beveiligd middels database encryptie. De audit trail en het GxP compliancy middelen ondersteunen hierin.
- Er worden twee soorten wachtwoorden voor elk gebruikersaccount aangeboden: inlogwachtwoorden en ondertekening wachtwoorden.
- Validatie van sampledata, QC-validaties en mechanismen in de workflow.
- Versie-gecontroleerde analytische stamdatabeheer, audit trail op opdrachten/sampledata gedurende het gehele actieve werkproces en versiebeheer van stamdata.
- Audittrailing conform ISO 17025 specs.
- ISO17025 conforme distributie van berichten en archivering.
- De belangrijkste maatregel om de betrouwbaarheid van het diagnostische proces te borgen is gelegen in het feit dat de processen boven op het standaard platform volledig gemodelleerd worden naar het specifieke proces. Hiermee kunnen alle brongegevens met de daarbij getrokken analyse in versiebeheer worden opgeslagen.
- De oplossing biedt autorisatiemogelijkheden en out-of-the-box audittrail functionaliteit. Op basis van de autorisatie structuur wordt bepaald wie (op basis van groepen) toegang heeft tot welke specifieke gegevens. Een beheerder van het systeem kan toegang hebben tot de primaire opslagstructuur. Aanpassingen op dit niveau worden ook vastgelegd in de audit trail. Op deze wijze wordt de betrouwbaarheid van de data gewaarborgd.
- Our system is in full accordance with ISO/IEC 17025. All data entry are fully traceable. All access are secured. Access rules are defined with several levels and are customizable.

31. *In het geval u scenario 1 (SaaS) en/of scenario 2 (Outsourcing via System Integrator) aanbiedt en uw oplossing wordt ontsloten via een beveiligde internetverbinding, hoe is uw technische en organisatorische beveiliging geregeld (neem hierin o.a. mee de toegang, autorisatie en het voorkomen van ongeoorloofde toegang, monitoring)?*

Deze vraag is alleen beantwoord door de leveranciers die deze scenario's aanbieden.

Beantwoording:

- De verbinding met de applicatie wordt verzorgd door de hosting partner welke gebruik maakt van AWS als infrastructuur provider. De fysieke toegang valt onder de verantwoording van Amazon, de logische beveiliging wordt door de hosting partner verzorgd welke ISO27001 en SSAE 16 SOC-2 gecertificeerd is. Alle fysieke en netwerk toegang wordt 24/7 gemonitord en gelogd. Dit wordt ook aangegeven door een andere leverancier, die hier de audittrail voor gebruikt.
- Onderdeel van onze ISO27001 certificering en procedures (A09.1.1-POL Toegangscontrole Beleid). LDAP Membership, DATABASE Membership, OAuth en SAML als inlogmethoden wordt ondersteund. Het gebruik van uniek traceerbare accounts wordt afgedwongen en Multi Factor Authentication (MFA) - waarbij ten minste Two Factor Authentication (2FA) wordt afgedwongen - is optioneel mogelijk. Als Federated Security wordt gebruikt, moet de NVWA zelf een ADFS en federaties met de andere partijen opzetten. De oplossing kan ook verbinding maken met meerdere SAML providers, maar de eindgebruiker moet dan zelf de juiste keuze maken uit de beschikbare manieren om in te loggen.
- Database Lidmaatschap: gebruikers en autorisatieregels worden opgeslagen in de database die door de applicatie wordt gebruikt.
- LDAP Membership: gebruikers en groepen worden beheerd in Active Directory. Autorisatieregels worden toegewezen aan de Active Directory (AD) Groepen en deze worden opgeslagen in de database die door de applicatie wordt gebruikt;
- Gebruikers dienen in te loggen met een persoonlijke gebruikersnaam en wachtwoord. Daarbij kan door middel van rollen, rechten en groepen worden bepaald wie, wat, wel of niet, mag doen en zien. De gebruikers en functionele onderdelen kunnen worden beveiligd met: rollen, taken, operaties (3 niveaus) die ook kunnen worden gegroepeerd. Hiermee kunnen we functionele onderdelen met verschillende operaties beveiligen en bieden we een zeer granulair beveiligingsmodel in het toewijzen van rollen aan gebruikers.
- De toegang tot informatie kan worden beperkt door lees/schrijf/bewerkingsrechten te geven op de onderliggende entiteit. Aan gebruikers kunnen bepaalde competenties (kwalificatie en geldigheid) en groepen worden toegewezen om te beheren welke gegevens een gebruiker kan zien.

- Monitoring wordt standaard aangeboden indien wij de oplossing hosten. Indien de NVWA zelf wil hosten kunnen deze diensten in overleg ook aan de NVWA worden geboden.
- Monitoring is gericht op de instandhouding van het platform en staat borg voor de beschikbaarheid van de applicaties, systemen en netwerkcomponenten. De daadwerkelijke beschikbaarheid van de informatiesystemen en de prestaties zijn van een groot aantal factoren afhankelijk en kunnen indien gewenst op specifieke manieren worden gemeten en gerapporteerd.
- Technische en organisatorische maatregelen zijn onderdeel van het overeen te komen SLA.
- Fysieke toegangscontrole tot Datacenter.
- Toegangscontrole gebruikers, gegevenstoegang, invoercontrole, opdrachtcontrole, beschikbaarheidscontrole en controle op gegevensscheiding.
- The solution is accessible through a secure login and password. It is possible to have a double login for more security (email or sms). It is possible to set a policy for the passwords, strength, validity or to have an SSO.
- De manier waarop het platform omgaat met authenticatie en autorisatie, staat in eerdere antwoorden beschreven. Het platform en de bijbehorende dienstverleningsorganisatie is standaard BIO compliant ingericht. Dit wordt ondersteund door een standaard DAP, SLA, Solution Architectuur en beveiligingsplan en team van medewerkers waarbij deze kennis geborgd is: compliance is meervoudig aangetoond door middel van audits.
- De applicatie wordt 24\*7 gemonitord door het Security Operation Center (SOC) en is alleen toegankelijk conform de afgesproken standaarden. Bij een poging tot ongeoorloofde toegang wordt dit geregistreerd in het SOC. Standaard zal de FortiWeb omgeving deze poging blokkeren en wordt het team over de poging geïnformeerd. Afhankelijk van het type melding wordt een handmatige verificatie uitgevoerd.
- Periodiek wordt gerapporteerd over de incidenten.

32. *In het geval u scenario 2 (Outsourcing via System Integrator) en/of scenario 3 (twee kavel pakket en System Integrator) aanbiedt en de oplossing wordt aangeboden vanuit een datacentre, hoe heeft u uw technische en organisatorische beveiliging geregeld (neem hierin o.a. mee de toegang, autorisatie en het voorkomen van ongeoorloofde toegang, monitoring)?*

Bij een aantal leveranciers komt het antwoord overeen met vraag 31.

Beantwoording:

- Er zal gehandeld worden conform afspraken datacentre waar zowel scenario 2 als 3 onderdeel van is. Monitoring vindt alleen plaats op cruciale onderdelen van de hardware en het operating system. Binnen het project en in lijn met afspraken worden deze set onderdeel van onze dienstverlening en governance afspraken en ingebed als uitgangspunt voor onze dienstverlening. Daarop zullen onze specialisten dan ook

vervolgens handelen en zullen we in het kader van informatiebeveiliging toezicht houden.

- De verbinding met de applicatie wordt verzorgd door de hosting partner welke gebruik maakt van Amazon AWS als infrastructuur provider. De fysieke toegang valt onder de verantwoording van Amazon, de logische beveiliging wordt door de hosting partner verzorgd welke ISO27001 en SSAE 16 SOC-2 gecertificeerd is. Alle fysieke en netwerk toegang wordt 24/7 gemonitord en gelogd.
- Technische en organisatorische maatregelen zijn onderdeel van het overeen te komen SLA.
- Fysieke toegangscontrole tot Datacenter.
- Toegangscontrole gebruikers, gegevenstoegang, invoercontrole, opdrachtcontrole, beschikbaarheidscontrole en controle op gegevensscheiding.
- The solution is accessible through a secure login and password. It is possible to have a double login for more security (email or sms). It is possible to set a policy for the passwords, strength, validity or to have an SSO. All access can be monitored and stored through the use of the audit trail.
- In het geval van scenario 3 zullen wij de dienstverlening onderbrengen bij DICTU en wordt de dienst ontsloten conform de richtlijnen van DICTU.

*33. Kunt u toelichten welke passende maatregelen u kunt bieden bij de verschillende dataclassificatie niveaus? Voor de definitie van classificatieniveaus verwijzen we naar: <https://bio-overheid.nl/>.*

Samenvatting:

Door meerdere leveranciers wordt aangegeven dat op basis van rollen, rechten en groepen zodanig geconfigureerd kan worden dat de verschillende dataclassificatie niveaus gerespecteerd worden. Een (1) leverancier geeft aan dat de klant hier ook een rol in heeft.

Beantwoording:

- Classificatie is vastgelegd binnen de oplossing, de modules dwingen dit af. In de database kan alleen gekeken worden met behulp van een account conform MS SQL rechtenstructuur.
- In combinatie met de procedures en kwaliteitssystemen van een klant wordt er een configureerbare oplossing geboden die een conforme en gevalideerde omgeving kan bieden voor de gebruikte functies. Met uitgebreide auditing, review functionaliteit en systeem controles, is aangetoond dat deze implementaties voldoen aan de eisen van agentschappen zoals de FDA, MHRA en WHO in GMP en GLP laboratoria.
- Door de toevoeging van een specifieke regulatory data integrity module (RDI) zijn de meeste klanteisen nu beschikbaar als gestandaardiseerde out-of-the-box functies, met gedetailleerde en uitgebreide opties voor het controleren van auditing, review, elektronische handtekeningen, gegevensregistratie, gegevensimport en meer. Voldoen aan alle aspecten

van de ALCOA+ principes kunnen voldoen, zodat alle gegevens op de juiste manier kunnen worden vastgelegd en onderhouden.

A = Toerekenbaar - wie een activiteit heeft uitgevoerd en wanneer

L = Leesbaar - kunnen alle gegevens (elektronisch en papier) zonder dubbelzinnigheid worden gelezen

C = Gelijktijdig - gedocumenteerd op het moment van de activiteit

O = Origineel - originele waarnemingen of een voor eensluidend gewaarmerkt afschrift

A = Nauwkeurig - geen fouten of wijzigingen zonder de juiste documentatie

Compleet - alle records bestaan voor de betreffende steekproef(en) en batch.

Consistent - de volgorde van activiteiten en gebeurtenissen volgt een verwachte volgorde.

Duurzaam - records worden opgenomen op een geautoriseerd medium.

Beschikbaar - records zijn toegankelijk gedurende de levensduur van de record (d.w.z. recordretentieperiode).

- Conformeren aan de eisen voor informatieveiligheid zoals tier 3/4 classificatie en certificering conform NEN-ISO 27001 (ISO 17021 en ISO 27006) van het Datacenter en werkend volgens de praktijken in overeenstemming met ISO27002.
- Op basis van de resultaten van de Quick Scan / PIA zullen de gegevens op het onderkende basisbeveiligingsniveau worden beveiligd.

*34. Heeft u ervaring met de ICO-wizard (Inkoopeisen Cybersecurity Overheid) op bio-overheid.nl? Zo ja, welk advies wilt u ons meegeven als wij dit gebruiken als basis voor het specificeren van de IB eisen voor deze oplossing?*

Samenvatting:

Geen enkele leverancier heeft ervaring met de ICO wizard. Er wordt ook geen bezwaar gemaakt tegen het gebruik ervan. Als advies wordt meegegeven indien de NVWA de ICO wizard wil toepassen het belangrijk is om vast te stellen of de set eisen volledig aansluit op de gevraagde dienstverlenings-variant Een leverancier geeft aan wel ervaring te hebben met het voldoen aan de BIO.

De vragen van paragraaf 1.5 en 1.6 zijn vertrouwelijk, de antwoorden worden niet gedeeld.

### **1.5 Samenwerking en ervaringen**

*(de beantwoording van deze vragen wordt niet gedeeld met andere partijen/vertrouwelijk)*

*35. Het streven van de NVWA is om zoveel mogelijk ontzorgd te worden.*

*Daarnaast is de NVWA op zoek naar een partij die aandacht heeft voor professionele doorontwikkeling. Wat voor samenwerkingspartner kan uw bedrijf zijn?*

36. Heeft u ervaring met soortgelijke opdrachten? Zo ja

- a. Voor deze soortgelijke opdrachten, om welke soortgelijke klanten gaat het? De NVWA behoudt zich het recht voor met betrekking tot opgegeven klanten, navraag te doen bij de betreffende opdrachtgever(s) over de tevredenheid.
- b. Geef daarbij aan per klant wat uw ervaring is.
- c. Geef aan per klant of u deze opdrachten zelfstandig heeft uitgevoerd, met behulp van onderaannemers of in een samenwerkingsverband. Neem hierin de taakverdeling mee.

#### **1.6 Prijsmodel**

(de beantwoording van deze vragen wordt niet gedeeld met andere partijen/  
vertrouwelijk)

37. Uit welke elementen bestaat het prijsmodel voor het door u aangeboden scenario('s)?
38. Als u kijkt naar onze eisen en wensen, met welke jaarlijkse kosten dient rekening gehouden te worden en wat is de totale investering voor een periode van 10 jaar?
39. Welke onderdelen adviseert u ons separaat op te nemen in een prijzenblad, om de kosten van inschrijvingen op een juiste wijze met elkaar te kunnen beoordelen?

#### **1.7 Gunningscriteria**

40. Op welke wijze is er een onderscheidend vermogen ten aanzien van de verschillende LIMS systemen of dienstverlening en wat zouden relevante en onderscheidende gunningscriteria zijn, die hierbij passen?

Beantwoording:

- De wijze waarop de leverancier kan schakelen met de ontwikkelaar binnen de tijdslijnen van het project en met duidelijke resultaatverplichting.
- Hoe organiseert en borgt de LIMS leverancier de oplossing waarbij nu voor 80% de inrichting is vastgelegd buiten het huidige LIMS.
- Lange termijn ondersteuning van een systeem door de leverancier. Hierbij rekening houdend met end-of-life systemen door bijvoorbeeld veranderende technologie (continuïteit).
- Eén software product (platform) i.p.v. diverse losse modules.
- Gratis upgrades en updates.
- Continue incrementele verbeteringen o.b.v. 2-wekelijkse releases (Continuous Delivery).
- Responsive web design wordt door 2 leveranciers aangegeven.
- 100% web gebaseerde technologie.
- Consultants in loondienst (geen freelancers) en hun ervaring.
- Mate van zelfwerkzaamheid van key-users in het gebruik.
- Applicatiefunctionaliteiten i.o.m. ISO 17025 reguleringen.
- identify the main aspects.
- When choosing a "classical" lims check the price of additional devs.

- Completeness of the solution (closeness to standard app).
- Coverage of actual/future needs.
- Aansluiting van de oplossing en dienstverlening op de standaarden voor overheidsdienstverlening (BIO, AVG, WCAG, archiefwet, Open standaarden forum voor standaardisatie etc.).
- Bewezen oplossing en dienstverlening binnen de overheid.
- Aansluiting op componentenlandschap en architectuur van de NVWA.
- Flexibiliteit en aanpasbaarheid van de oplossing wordt door 3 leveranciers genoemd.
- Time to Market voor aanpassingen.
- Best of Breed.
- Hergebruik.

*41. Op welke wijze kan innovatief en maatschappelijk verantwoord inkopen een rol spelen bij deze aanbesteding?*

Samenvatting:

Innovatie en maatschappelijk verantwoord ondernemen (MVO) is een belangrijk thema voor alle leveranciers.

Beantwoording:

- Door het creëren van een duurzame relatie tussen leverancier en opdrachtgever.
- Innovatie: bijdrage aan het goedkoper, duurzamer, sneller, betrouwbaarder en veiliger uitvoeren van de publieke taken van de NVWA.
- Milieu : Volledig papierloos werken
- Conformereren aan de maatschappelijke eisen ter voorkoming van misstanden in de arbeidsmarkt.
- Aandacht geven aan social return, door middel van maatschappelijk vriendelijk personeelsbeleid.