Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

AANVRAAGFORMULIER **RISICOACCEPTATIE**

.

Betreft:	LCC Dashboard fase 2 (o.b.v. Microsoft Azure inrichting)	
Aanvrager:	5.1.2e 5.1.2e ; 5.1.2e 5.1.2e	
Begeleider risicoacceptatie vanuit CISO team:	5.1.2e 5.1.2e	
Aanvraagnummer:	20210331-02 RACC LCC Dashboard fase 2	
Datum aanvraag:	31-03-2021	
Centrum/dienst:	Logistiek Coördinatiecentrum Covid vaccinatie (LCC)	
Systemen	Managementinfo • Dataplatform in MS-AZURE CLOUD (RIVM-tenant) • Datavirtualisatieplatform RIVM/SSCC (=Tibco) • Reportservers Power BI RIVM/SSCC	
• Verantwoordelijk lijnmanager:	• 5.1.2e 5.1.2e 5.1.2e	
Verantwoordelijk centrum- of afdelingshoofd:	• 5.1.2e 5.1.2e 5.1.2e , 5.1.2e	• 5.1.2e 5.1.2e 5.1.2e , 5.1.2e 5.1.2e
Informatiemanager:	5.1.2e 5.1.2e	5.1.2e 5.1.2e
• Doel:	• Vaststellen risico's en te nemen maatregelen c.q. uit te stellen maatregelen	
• Aan:	• 5.1.2e 5.1.2e , 5.1.2e • 5.1.2e 5.1.2e 5.1.2e , 5.1.2e • 5.1.2e 5.1.2e 5.1.2e , 5.1.2e • 5.1.2e 5.1.2e , 5.1.2e	
• T.b.v. vergadering:	• Via e-mail	
• Aantal pagina's:	• 11	
• Notitie toegevoegd:	• Geen	
• Versienummer:	• 0.2	
• Datum laatst gewijzigd:	• 07-04-2021	

• **Quickscan resultaat COVID-19 vaccin bestelproces** • *Neem hier de resultaten van de Quickscan over*	Datum Quickscan BIO: 23 februari 2020

I	Samenvatting											
	STAP 1		STAP 2				STAP 3					
	(X)	Rubricering	(X)	Classificatie proces	(X)	Classificatie systeem	(X)	B	(X)	I	(X)	V
		Openbaar		Ondersteunend		Nuttig		Laag		Laag	X	Laag
		RIVM Intern (besloten)		Bijdragend	X	Belangrijk	X	Midden		Midden		Midden
	X	RIVM Vertrouwelijk		Strategisch	X	Vitaal	X	Hoog	X	Hoog		Hoog
		Departementaal Vertrouwelijk	X	Kritisch strategisch								
		Staatsgeheim Confidentieel										
		Staatsgeheim Geheim										
		Staatsgeheim Zeer Geheim										

BBN *1, 2, 3 of VIR-BI*	*2*	*BBN2:* *Logistieke data mbt voorraad, scenario's en (uit)levering van vaccins en toebehoren* *Data van het supportcentrum COVID over logistieke vragen mbt leverlagen vaccins*

Proces: Het proces is geclassificeerd als 'kritisch strategisch' want de output van het proces is input voor VWS dashboarding en wordt doorgestuurd naar VWS. M.b.t de planning is deze informatie input voor besluitvorming (NB op basis van besluitvorming wordt feitelijke bestelling gedaan).

Systeem: Het dataplatform in Microsoft Azure (dedicated RIVM-tenant) is Vitaal. Zonder input van het dataplatform is het niet mogelijk om tijdig en beheersbaar het proces te kunnen draaien. Het data virtualisatieplatform en de reportservers Power BI (beide hosting bij RIVM/SSCC) zijn Belangrijk. Omdat het batchverwerking betreft, is een handmatig alternatief mogelijk.

Informatie: Omdat we in een crisissituatie zitten is de eis voor beschikbaarheid Hoog voor het dataplatform. Voor de overige systemen is dit Midden. De integriteit is Hoog omdat het direct samenhangt met de integriteit van het vaccinatieprogramma. Informatie blijft eerst nog binnen de politiek maar wordt uiteindelijk openbaar wat maakt dat de vertrouwelijkheid Laag is.

Voor wat betreft de nadere onderbouwing van de vertrouwelijkheiod, zie onderstaande toelichting op data ten behoeve van de KPI's:

Kpi's	*Vertrouwelijkheid informatie*	*Integriteit informatie*	*Beschikbaarheid informatie*
Voorraad vaccins	Niet. Informatie wordt al gepubliceerd in tweede kamer briefings en op VWS dashboard.	Van groot belang. Als er sprake is van manipulatie door statelijke actoren dan wordt dat eruit gehaald vanwege: Vierkantscontroles die worden uitgevoerd. Vier ogen principe; vergaande kennis van direct betrokkenen in LCC (Current en Plans, afdelingen verantwoordelijk voor resp. uitlevering en planning). Azure controles die manipulatie detecteren.	Van groot belang. Het gaat om essentiële sturingsinformatie voor interne partijen (Programma als geheel en LCC in het bijzonder) en externe partijen (VWS en uitvoeringspartners) betrokken bij de uitvoering van het covid vaccinatieprogramma.
Toeleveringen vaccins	Niet. Informatie wordt al gepubliceerd op RIVM-, VWS- en ECDC dashboard		
Uitgeleverde vaccins naar uitvoerings-partners	Niet. Informatie wordt al indirect gepubliceerd op VWS dashboard in vorm van proxi van EPI van gevaccineerden incl. berekeningen. Idem voor ECDC dashboard.		
Toeleveringen toebehoren	Niet. Informatie wordt nu niet gedeeld, omdat daar nog geen mogelijkheden voor zijn.		
Voorraad toebehoren	Niet. Informatie wordt nu niet gedeeld, omdat daar nog geen mogelijkheden voor zijn.		
Uitleveringen toebehoren	Niet. Informatie wordt nu niet gedeeld, omdat daar nog geen mogelijkheden voor zijn.		
Scenario's uitleveringen	Niet. Scenario's worden verwerkt in Tweede Kamer briefings.		
Operationele planning	Niet. Operationele planning wordt extern gedeeld met uitvoeringspartners en VWS, die het weer gebruikt voor onder meer Tweede Kamer briefings.		

- **Aanleiding**

Gerelateerd proces of informatiesysteem (+doelstelling)

- *Korte omschrijving van proces(sen) en informatiesyste(e)m(en) waar de risicoacceptatie betrekking op heeft en de doelstelling ervan*

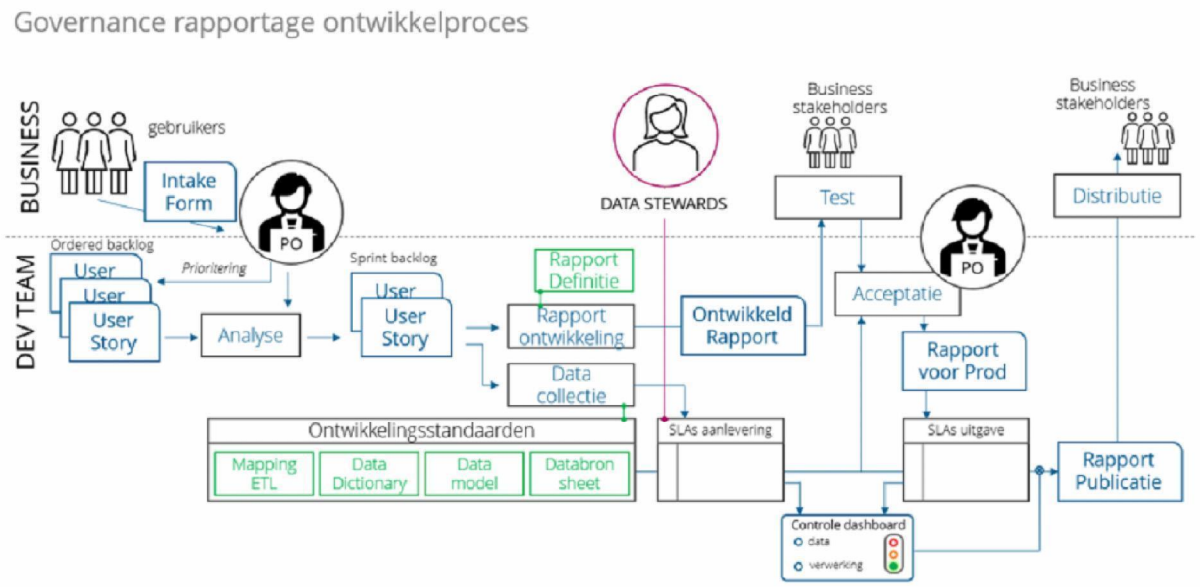
In januari'21 startte het landelijke vaccinatieprogramma Covid, het grootste vaccinatieprogramma van Nederland ooit. Eén van de kritische processen om dit programma effectief uit te voeren is het logisitieke en operationele proces.

Bijzonderheden van het COVID vaccin:
* schaarste: beperkte beschikbaarheid vaccins bij de start;
* verschillende merken vaccins: specificaties, gebruiken effectiviteit naar doelgroepen;
* vaccinatiestrategie naar doelgroepen (advies Gezondheidsraad);
Gevolg: gefaseerde implementatie met in eerste instantie aanbodsturing (ipv vraagsturing).
Dit traject is een deeltraject van het Landelijk Coordinatiecentrum COVID vaccinatie die als doelstelling heeft: "Effectief organiseren en coördineren van de goederenstroom en dienstverlening van A naar B. Aanbod en vraag afstemmen."
Eén van de kritische onderdelen daarbij is het beschikbaar stellen van tijdige en adequate informatie die uitvoerders en beleidsmakers in staat stelt om de juiste acties te kunnen ondernemen.
Er is een acute behoefte om managementinformatie rond vaccinleveringen (en toebehoren) inzake het COVID-programma op te leveren. Het betreft informatie over voorraden planning en levering en distributie van vaccins, naalden, spuiten, diluent en overige relevante artikelen.

Deze informatie moet de uitvoering en beleidsmakers gaan ondersteunen met tijdige en juiste informatie. De informatie kan op verschillende wijzen worden gepresenteerd:
- Inzicht in (management) informatie via Dashboards (doelgroep rapportages)
- (Publieke) Data aanlevering aan (externe) sites (o.a. COVID-19 dashboard)
- Data Storytelling

Hiertoe moet een platform worden ingericht om de hiervoor benodigde data te kunnen verzamelen, beheren en op een veilige wijze te kunnen verwerken. Daarnaast moeten processen worden ingericht om die data op een juiste wijze te kunnen leveren, verwerken en publiceren.
De doelstelling is om op zo kort mogelijke termijn een adequate voorziening te realiseren.

Schematische weergave v/h proces rond beheer/ontwikkeling Managementinformatie:

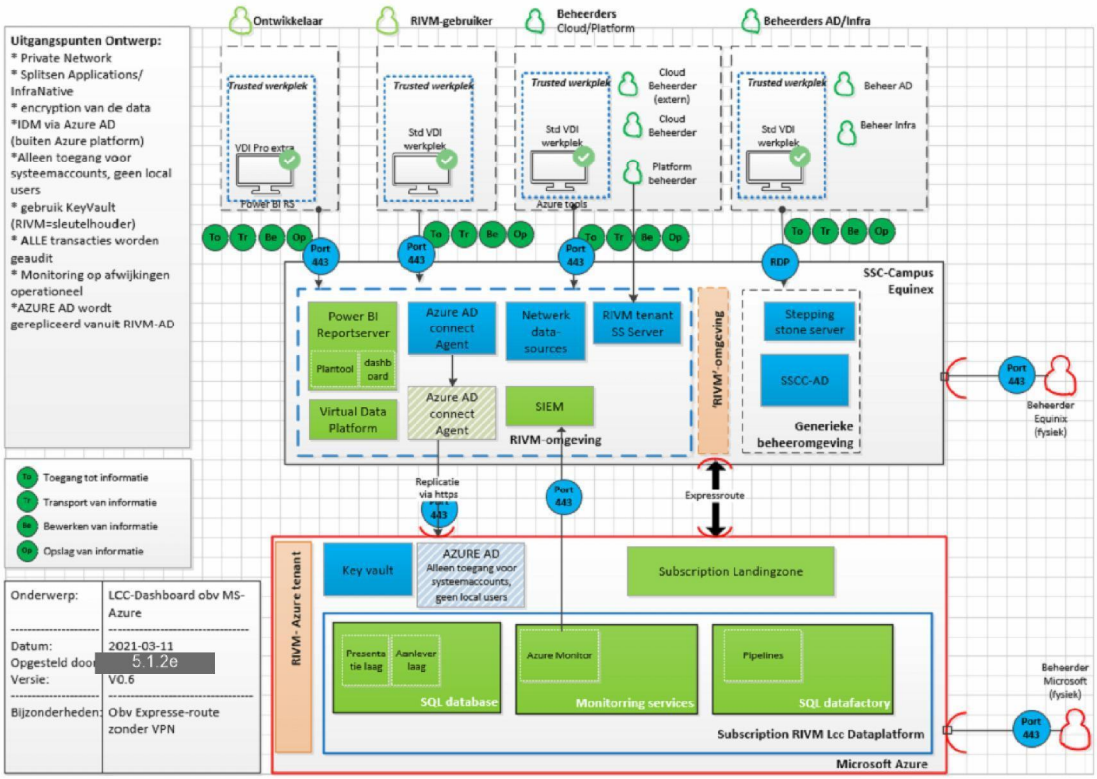


Proces	Toelichting
Aanlevering bronbestanden	Op basis van vragen van de business wordt een intake gedaan en geanalyseerd welke data(bronnen) nodig zijn. Indien nodig (bv bij gebruik van hoger geclassificeerde data) zal een risico-check worden uitgevoerd. Er zal worden gewerkt met standaarden (datasheets, dictionary, data-SLA's etc) om de dataflow tm distributie eenduidig vast te leggen.

Beheer en ontwikkeling Managementinformatie	O.b.v. de analyse wordt een rapport ontwikkeld. Hier worden ontwikkelingsstandaarden toegepast. Een ontwikkeld rapport wordt ter acceptatie voorgelegd aan de stakeholders
Beheer Datamodellen en datastromen op Azure platform	Dit wordt gedaan conform de standaarden die opgesteld zijn door ViqtorDavis-DeltaN
Beheer Datamodellen en datastromen op Tibco Platform	Dit wordt gedaan conform de standaarden die opgesteld zijn door IV (Beheer Tibco-platform)
Beheer gepubliceerde rapporten	Vrij gegeven rapporten worden beheerd door DVP/LCC-rapportage team. Er wordt een controle-dashboard ingericht om de datastroom en verwerking dagelijks te kunnen monitoren.

Rijksinstituut voor Volksgezondheid
en Milieu
Ministerie van Volksgezondheid,
Welzijn en Sport

Systeemdecompositie LCC Dashboard - fase 2
Systeemdecompositie van het betreffende informatiesyste(e)m(en)



Vanuit de SSC Campus beheeromgeving wordt via een (beveiligde) expressroute verbinding de dedicated RIVM tenant ontsloten. Authenticatie verloopt via de Azure AD koppeling.

Data vanuit operationeel proces LCC worden verzameld en via het Virtual Data Platform naar een Azure-RIVM-tenant gezet en verwerkt voor gebruik in een dashboard via Power BI en gepubliceerd op de RIVM-interne reportserver PowerBI.

Voor het Virtual Data Platform 5.1.2e en de inzet van PowerBI-servers zijn in het kader van CIMS-BI al risico-analyses uitgevoerd. Dit project maakt gebruiken van dezelfde infrastructuur. De processen en beheer rond/van deze onderdelen worden hier verder niet uitvoerig behandeld.

- **Informatiebeveiliging en risico's**

15 februari is in een ingelaste meeting met 5.1.2e 5.1.2e en 5.1.2e over de dataclassificatie van de uitkomsten van de quickscan BIO i.r.t. tot de requirements vanuit het VWS cloudbeleid* besproken en is de classificatie voor de verwerkte informatie vastgesteld op RIVM Vertrouwelijk en het basisbeveiligingsniveau op 2 (BBN2). De verwerkte informatie betreft de geaggregeerde infomatie vanuit het bestelproces en heeft niet het dreigingsniveau van de inhoudelijke bestelinformatie.

Naast het VWS cloudbeleid is tevens het NBV (AIVD) standpunt public-clouddiensten en gerubriceerde gegevens (januari 2021) meegenomen in de overweging:
"Bij uitbesteding van informatiesystemen naar een public cloud adviseert het NBV de manager om de risico's en kansen van

de uitbesteding te analyseren, de gevolgen voor de organisatiedoelstellingen te beoordelen, de naleving van geldende wet- en regelgeving te toetsen en de bijbehorende risico's beheersbaar te maken. Hierbij dienen de voor- en nadelen van publicclouddiensten en "on premise" oplossingen te worden vergeleken en de dreiging van onder andere Advanced Persistent Threats (APT's) te worden meegewogen."
Voorts geeft ze aan:
"Mocht de ICT-dienstverlener echter gehinderd worden door groeiende complexiteit van de infrastructuur gecombineerd met legacy-problematiek, dan zal hij de snelle ontwikkelingen op ICT-gebied en de groeiende behoeftes van de organisatie minder goed kunnen volgen. Als de ICT-dienstverlener daarbij de groeiende cyberdreigingen niet kan bijhouden, dan kan dit risico's opleveren voor de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT-infrastructuur. In dergelijke situaties is het niet uitgesloten dat public-clouddiensten de ICTinfrastructuur veiliger, wendbaarder en kosteneffectiever kunnen maken. Clouddienstverleners leveren nu al innovatieve ICT-diensten die moeilijk in eigen beheer te bouwen zijn. Clouddienstverleners kunnen door schaalgrootte, automatisering en inzet van kunstmatige intelligentie in sommige gevallen betere beveiliging bieden dan de eigen ICT-dienstverlener."

Op 19 februari hebben meetings plaatsgevonden waarbij Microsoft toelichting gaf over de ervaringen die zij hebben samen met overheidsdiensten in relatie tot het gebruik van hooggeclassificeerde data op MS AZURE. Verder werden aandachtspunten besproken en de (rest)risico's waar rekening mee moet worden gehouden.
Begin maart is de systeemdecompositie door VD&D opgesteld en vervolgens in een aantal sessies de risicoanalyse uitgevoerd en uiteindelijk deze risicoacceptatie opgesteld.

Privacy

De betrokken data bevat geen bijzondere persoonsgegevens.
Er hoeft geen DPIA te worden uitgevoerd.

- **Probleemstelling, risicobeschrijving en mitigatie**

Geef hierbij aan welk risico geaccepteerd wordt dan wel voor welk beleid een ontheffing aangevraagd wordt. Geef duidelijk aan wat het risico is, welke mitigerende maatregelen getroffen zijn en wat het managed risico is

Er is hoge noodzaak voor een korte termijn oplossing waar gebruik kan worden gemaaktg dat voor het gebruik van clouddiensten vanuit VWS beleid een aanbevelingen van bijv. NBV (AIVD) meer is. Toegestaan. Het gebruik van Microsoft Azure is nieuw voor het RIVM en SSC Campus tevens is het Cloud Competense Center (CCC) in oprichting.

Algemene eisen vanuit informatiebeveiliging voor clouddiensten zoals deze zijn een goed cloudbeheer en goed ingericht CCC, het key management (sleutelbeheer) bij RIVM (SSC Campus) en een goede inrichting van IT security beheer (dit is niet gelijk aan IT beheer). Deze punten zijnopgenomen in het beheerplan.

Door Microsoft is op 24 maart 2021 een peer review uitgevoerd. Scope was de inrichting van de MS-Azure tenant RIVM tbv Dataplatform LCC-Dashboard.

Aanbevelingen vanuit Microsoft:
De Microsoft presentatie en het document met de aanbevelingen is nog niet beschikbaar gesteld. Op basis van de aantekening zijn de volgende aanbevelingen benoemd: (PO=onderdeel van project)

Aanbeveling	Omschrijving	Uitvoering als Onderdeel project / status
1. Development (O/T/A?) - omgeving	Acties zijn in werking gesteld om een 'development' omgeving vóór live-gang beschikbaar te hebben.	Ja / Vrijdag 2-4 gereed
2. Keyvault	Dit betreft het dichtzetten van toegang voor developers tot de productie-omgeving.	Ja / Gereed
3. DNS	Dit betreft het hanteren van hostfile op de servers ipv. centrale DNS voor name resolving	Nee(Niet urgent) Bij inrichting LCC
4. Externe toegang	Wordt dicht gezet voor externe toegang van gebruikers. Om na te kunnen gaan welke mogelijkheden er zijn om de externe toegang dicht te zetten voor	Ja / Deels gereed [1)] Deels bij inrichting CCC [3)]

	beheer, zonder ongewenste impact op MS Teams en MS 365 moet er een duidelijk 'plaatje' komen.	5.1.2e diagram opstellen van Azure cloud met daarin dataplatform, MS Teams en MS 365 [2)]
5. Firewall	Vandaag zijn de benodigde wijzigingen hiervoor doorgevoerd, in afstemming met VD&D (via 5.1.2e	Ja / Gereed
6. Disaster recovery	In eerste instantie is er een advies nodig tbv. besluitvorming voor verder vervolg door management IV(CCC)	Nee(Niet urgent) Bij inrichting CCC
7. Automated configuration	In eerste instantie is er een advies nodig tbv. besluitvorming voor verder vervolg door management LCC	Nee(Niet urgent) In vervolgtraject LCC

[1)] *In de huidige inrichting is het niet mogelijk dat technische cloud beheerders bij de data kunnen. Functionele beheerders kunnen alleen vanuit on-premise omgeving bij de data komen maar niet bij de technische Azure inrichting. Deze scheiding is ook doorgevoerd in de verschillende subscriptions waarbij technische beheerders alleen de hun toegewezen omgeving kunnen beheren.*

[2)] *In een van de risico sessies met 5.1.2e hebben we een tekening laten zien van de verbindingen. Op deze tekening stonden de verbindingen niet. Echter 5.1.2e gaf aan dat de door ons getoonde tekening niet overeenkomt met de template voor de systeemdecompositie en deze is tevens gemaakt. Als we nu de huidige tekening uitbreiden met de management APi's en de verbindingen hiertussen is het van belang dit ook mee te nemen in de systeemdecompositie..*
De cloudarchitect zal het initiatief nemen om vanuit het CCC met 5.1.2e gaat overleggen hoe de beveiliging binnen cloud omgevingen werken en hoe we het beste met triggers om kunnen gaan.

[3)] *Voor technisch beheer is een best practice om naast login en wachtwoord ook MFA in te richten. Uit het bevindingen rapport kwam naar voren dat dit niet het geval is. We doen onderzoek naar de impact van MFA op de management omgeving van Azure.*

- **Risicomatrix**

Geef in de matrix aan waar het risico zich bevindt (dit op basis van de risicoanalyse; in te vullen door CISO of FCC/S&S)

Status risico's LCC dashboard fase 2 voor migratie:

Risicomatrix					
kans impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)					
2 (midden)	R21		R01 R12 R14 R19 R20 R25		
1 (laag)	R02 R04 R07 R09 R15 R23 R24		R03 R05 R06 R08 R10 R11 R13 R16 R17 R18 R22		

Status risico's LCC dashboard fase 2 na mitigatie:

Risicomatrix					
kans impact	1 < 1 keer per 10 jaar	2 Minimaal 1 keer 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 (hoog)					
2 (midden)	R21	R01 R12 R14 R19 R20 R25			
1 (laag)	R02 R04 R07 R09 R15 R23 R24		R03 R05 R06 R08 R10 R11 R13 R16 R17 R18 R22		

Overzicht inhoudelijke risico's

•	• Risico Ref.	• Maatregel besproken tijdens RA	• Gerelateerde BIO norm	• Status • *(CISO RIVM)*	• Bijzonderheden • *(CISO RIVM)*
R01	**Gebruik van de onrechtmatig verkregen inloggegevens van een medewerker of andere belanghebbende; zowel binnen RIVM als bij ketenpartner.**	- Vanuit AIP koppeling Azure monitoring met SIEM Agent binnen de Azure om verdacht verkeer te detecteren. - Encryptiesleutels in eigen beheer. CvZ: Gebruik van Azure Security Center en Azure defender : https://azure.microsoft.com/en-us/services/security-center/	**9.3.1** **9.4.2.1**		
R12	**Fouten door foutgevoelige/complexe bediening**	- Goede werkinstructies en training.	**12.1.1**		
R14	**Fouten door onvoldoende kennis/training; het borging van kennis**	- Goede werkinstructies en training.			
R19	**Ontwerpfouten in de ontwikkeling van de software (waaronder evt. achterdeur in de programmatuur)**	- Er worden basis componenten gebruikt en er wordt vanuit architectuur gewerkt.	**14.2.1**		
R20	**Ongeautoriseerd mutaties doorvoeren (afstand overnemen van systeem)**	- Integriteitscontroles en audit trail.			
R25	**Ziektegolf door besmetting met virus of bacterie**	- Zorg dragen voor voldoende back-up van medewerkers bij het ontwikkelen en het beheer van het platform.			

Maatregelen verder uitgewerkt:	Gerelateerd risico	Opvolging	Verantwoordelijke
M01. Azure wordt ingericht met externe expertise (en met Microsoft)	**R12, R14, R25**	Beschrijving in doelarchitectuur	VD&D 5.1.2e 5.1.2e
M02. Agent binnen de Azure om verdacht verkeer te detecteren.	**R01**		
M03. Geen externe connecties toestaan	**R01**		

M04. Juiste monitoring inrichten (met tresholds op gebruik van systeemresources)	**R19**		
M05. Datamodel binnen Azure kent integriteitscontroles.	**R14**		
M06. Op het platform kunnen alleen vastgestelde services draaien. Betreft alleen door MS gecertificeerde software.	**R19**		
M07. Encrypted verbinding via express route en en to end toegepast	**R01**		
M08. Alle configuraties worden uitgevoerd/gewijzigd vanuit RIVM accounts (met 2FA)	**R01**		
M09. Conditional access toepassen	**R01**		
M10. Gebruik maken van autopatch cloud technologie	**R19**		
M11. Toepassen integriteitscontroles en audit trail	**R14**		
M12.Conceptueel ingericht externe toegang niet mogelijk is.	**R01, R20**		
M13. Gegevens achteraf nog beoordelen.	**R12**	Achteraf beoordeling: gebruikers dashboards	Gebruikers (inherent)
M14. Goede werkinstructies en training. Tussentijdse controles implementeren.	**R12, R14**	Werkinstructies en training meenemen in beheer.	5.1.2e (5.1.2e 5.1.2e 5.1.2e 5.1.2e)
M15. Integriteitscontroles en audit trail.	**R14**	Meenemen in beheer	
M16. Vanuit AIP koppeling Azure monitoring met SIEM	**R01**	Meenemen in beheer	
M17: Het inrichten van key management (sleutelbeheer) bij RIVM (SSC Campus) en een goede inrichting van IT security beheer (dit is niet gelijk aan IT beheer).	**R01, R20**	Meenemen in beheer	
M18. Contractuele afspraken met Microsoft.	**R01**	Contractafspraken MS: documentatie presenteren	5.1.2e (5.1.2e 5.1.2e 5.1.2e)
M19. Bewaken: Vanuit AIP koppeling Azure monitoring met SIEM	**R01**		

Mitigerende maatregelen niet van toepassing
Geef aan waarom geen additionele maatregelen getroffen kunnen worden en/of waarom het beleid niet geïmplementeerd kan worden
Geef dit bij voorkeur per risico aan

Niet van toepassing

- **Consequenties andere partijen**
- *Geef aan of andere partijen (domeinen, centra, leveranciers, klanten) consequenties kunnen ondervinden van dit risico*
- *Geef dit bij voorkeur per risico aan*

Mogelijke issues of incidenten kunnen de beeldvorming / het imago van de leveranciers (MS en ViqtorDavis/Delta-N) negatief beïnvloeden.

- **Periode**

Geef aan voor welke periode de risicoacceptatie moet gaan gelden en wat de einddatum van deze acceptatie is

Deze risicoacceptatie is de uitwerking van het besluit van 25 februari 2021 en geldig tot en met maandag 1 mei 2021. In de komende maanden zullen (continuerend en deels iteratief) nadere analyses en testen worden uitgevoerd.

- **Evaluatie**
- *Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden*

In doorloop zullen de komende weken bij uitbreidingen gap-analyses en risicoanalyses plaatsvinden, maatregelen geïmplementeerd en testen uitgevoerd worden en daarbij afstemming met de verantwoordelijken.
Relevante restrisico's worden geregistreerd in het risicoregister, de voortgang op mitigerende

maatregelen wordt actief bewaakt. Er wordt een coördinator aangesteld om het IB&P-proces te begeleiden en maatregelen te implementeren.

Gevraagd besluit:	**Akkoord te gaan met het accepteren van de benoemde (rest)risico's voor informatiebeveiliging zoals deze nu bekend zijn over het proces rond managementinformatie tbv LCC/ COVID vaccins**		
Partij	***Naam***	***Mening*** *(invullen door Hoofd centrum, CISO, CIO, Compliance, Legal, Privacy en DR)*	***Akkoord***
Hoofd DVP	5.1.2e 5.1.2e 5.1.2e		Akkoord: ja/nee
CISO *(mandatory voor alle risk levels)*	5.1.2e 5.1.2e		Akkoord: ja
Privacy Officer	Nvt		Akkoord: nvt
CIO *(mandatory voor medium en hoger risico)*	5.1.2e 5.1.2e 5.1.2e		Akkoord: ja/nee