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

AANVRAAGFORMULIER RISICOACCEPTATIE

Betreft:	COVID-19 Information and monitoring system CIMS
Aanvrager:	RIVM-DVP
Telefoonnummer:	
Aanvraagnummer:	20200902-02 RACC CIMS
Datum aanvraag:	6-1-2021
Naam verantwoordelijk lijnmanager:	5.1.2e
Naam centrum- of afdelingshoofd:	5.1.2e
Centrum:	DVP
Naam Informatiemanager:	5.1.2e
Doel:	Vaststellen risico's en te nemen maatregelen c.q. uit te stellen maatregelen
Aan:	5.1.2e (CISO RIVM)
T.b.v. vergadering:	Stuurgroep COVID registratie
Aantal pagina's:	6
Notitie toegevoegd:	CIMS_Issue_actielijst P_IB v1.9.xlsx
Versienummer	1.1
Datum laatst gewijzigd	6-1-2021

Context / resultaat quickscan

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		Laag
	RIVM Intern (besloten)		Bijdragend		Belangrijk		Midden		Midden		Midden
	RIVM Vertrouwelijk		Strategisch	X	Vitaal	X	Hoog	X	Hoog	X	Hoog
X	Departementaal Vertrouwelijk	X	Kritisch strategisch								
	Staatsgeheim Confidentieel										
	Staatsgeheim Geheim										
	Staatsgeheim Zeer Geheim										

Aanvullende opmerkingen of randvoorwaarden

Security:

- CIMS wordt gebouwd op een kopie van de Praeventis database.
- Praeventis heeft alle security risico's / maatregelen doorlopen. De eisen van CIMS zijn (behalve beschikbaarheid) niet hoger dus dit voldoet voor CIMS. Voor de beschikbaarheid zijn aanvullende maatregelen genomen.

Privacy:

- Voor CIMS is een uitgebreide DPIA uitgevoerd, waar de hier genoemde restrisico's ook in zijn meegenomen.

Aanvraagnummer
Geef aan onder welk nummer de aanvraag al in het risk register staat of dat het een nieuwe aanvraag betreft

20200902-02 RACC CIMS (nieuwe aanvraag)

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

CIMS is het landelijk centraal registratiesysteem voor de registratie van de COVID-19 vaccinatie. Het RIVM verzorgt o.a. de centrale registratie van binnenkomende berichten van zorgverleners die de vaccinaties zetten bij personen. Naast centrale registratie wordt CIMS gebruikt voor kwaliteitsmonitoring en rapportage, het kunnen nemen van maatregelen na constateren van bijwerkingen en het doen van recalls. Met registratie wordt de vastlegging van de vaccinatie bij een persoon bedoeld.

Het CIMS is gebouwd op een kopie van Praeventis. Praeventis verzorgt standaard de inkoop, opslag en registratie van vaccins en monitoring toediening vaccinaties. Behalve dat Praeventis de bovenstaande functies bevat, zijn ook de processen er omheen ingericht.

Het centrale registratiesysteem wordt gevoed vanuit verschillende bronsystemen van diverse zorgverleners.

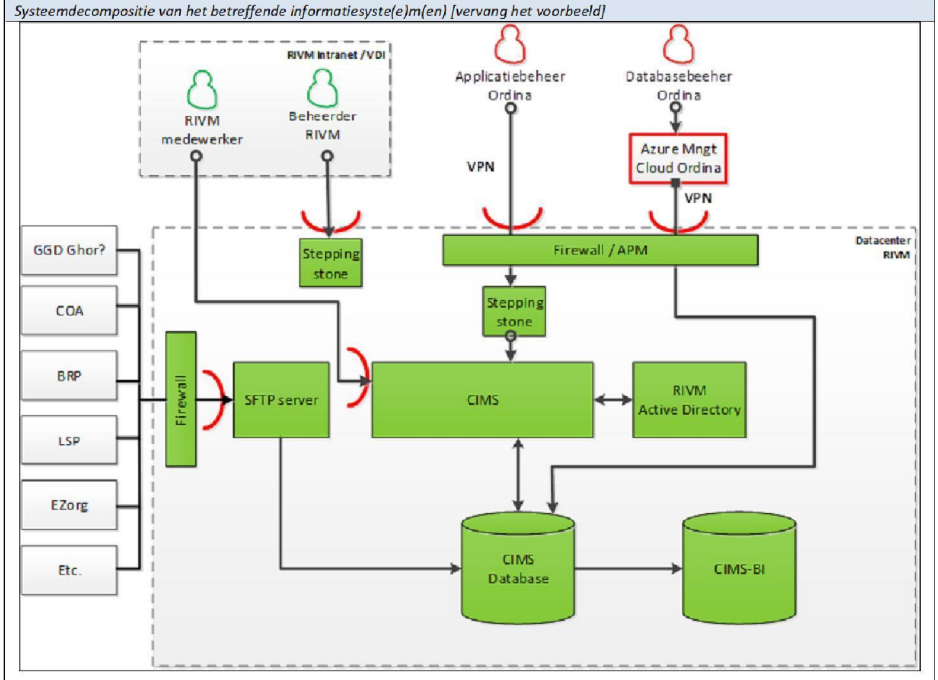
Risicoanalyse
Er is een risicoanalyse uitgevoerd op basis van de uitgevoerde quickscan, systeemdecompositie, workshops, interviews en documentatiereviews.

In de risicoanalyse zijn initieel de mogelijke risico's beschouwd. Hiervan zijn 49 risico's van toepassing verklaard op CIMS. Deze zijn samengevat in het bijgevoegde document ' CIMS_Issue_actielijst P_IB v1.8.xlsx'. Deze risico's zijn beoordeeld op kans en impact. Er zijn 44 risico's opgelost en/of niet van toepassing verklaard. Er zijn 5 risico's die nog niet zijn opgelost als CIMS in productie wordt genomen. Hiervoor zijn mitigerende maatregelen genomen om de kans op optreden van het risico zo laag mogelijk te maken.

Er zijn een drietal externe partijen (Noordbeek, ADR en Secura) die een aanvullende analyse hebben gedaan op een kleiner gedeelte van de systemen in scope; met name toegespitst op de SFTP server die een verbinding heeft met internet en waar alle registratiegegevens op binnenkomen. De urgente bevindingen uit deze analyses zijn allemaal opgelost en adviezen worden meegenomen op de ontwikkelroadmap van CIMS.

Systeemdecompositie

Systeemdecompositie van het betreffende informatiesyste(e)m(en) [vervang het voorbeeld]



Risico's		**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*			
		Onderstaande tabel geeft de risico's weer die nog niet helemaal zijn opgelost als het systeem in productie gaat. Hiervoor zijn wel mitigerende maatregelen getroffen om de kans op optreden van het risico zo klein mogelijk te maken.			
Ref.	**Risico**	**Maatregelen**	**Gerelateerde BIO norm** *Geef hier aan welk BIO-norm van toepassing is*	**Status** *(CISO RIVM)*	**Bijzonderheden** *(CISO RIVM)*

R02	Geen two-factor authenticatie bij inloggen in de CIMS applicatie. Bij diefstal van inloggegevens (bijv. via phishing) zou een aanvaller eenvoudig kunnen inloggen in de CIMS applicatie.	- Voordat er ingelogd kan worden in de CIMS applicatie, moet een gebruiker eerst met two-factor authenticatie inloggen op de RIVM VDI omgeving. - Om vervolgens toegang te krijgen tot de applicatie moet er dan via de VDI apart worden ingelogd met een door DVP-BIS verstrekte persoonlijke login en wachtwoord. - VDI omgeving heeft geen koppeling met internet voor CIMS gebruikers. - Monitoren van verkeerde inlogpogingen.	9.1.2 9.4.1 9.4.2	Restrisico voor acceptatie	
R08	Aangeleverde CSV bestanden zijn zelf niet voorzien van encryptie. Bij (ongeautoriseerde) toegang tot de SFTP server zou men de aangeleverde databestanden kunnen inzien.	- Importeren van bestanden is geautomatiseerd; geen menselijk handelen noodzakelijk. - Aanlevering van bestanden verloopt via verbinding die wel voorzien is van encryptie. - Bestanden worden na aanlevering op de SFTP server meteen doorgezet voor import en verwijderd (automatisch). - Toegang tot de SFTP server wordt gelogd. - Eerste periode is geen gebruik van CSV bestanden. - Bij de koppeling met BRBA worden deze wel voorzien van encryptie	13.1.1 13.1.2 9.1.2	Restrisico voor acceptatie	
R33	Database is niet voorzien van encryptie. Een databasebeheerder (van Ordina) heeft toegang tot alle data in de CIMS database en kan alle gegevens inzien.	- De on- en offsite back up van de database zijn versleuteld. - Het aantal database administrators is beperkt. - Aantal beveiligingsschillen om de database maakt ongeautoriseerde toegang door een aanvaller bijna onmogelijk. - Contractuele afspraken met Ordina. - Logging van activiteiten door administrators (op persoonsniveau). - Controle van de logfiles (in eerste instantie handmatig, later automatisch). - Maandelijkse controle van toegangsrechten.	9.1.2 9.4.1 12.4.1 12.4.2 12.4.3	Restrisico voor acceptatie	
R36	Logging van activiteiten door databaseadministrators wordt handmatig en 1x per maand gecontroleerd. Ongeautoriseerde toegang door een databaseadministrator blijft maximaal een maand onopgemerkt.	- Het aantal database administrators is beperkt. - Logging wordt aangeleverd bij SIEM/SOC van het RIMV voor monitoring. - Handmatige controle van lograpportage (wekelijks in de eerste maand na live gang). - Na in productie name van CIMS wordt monitoring geautomatiseerd, zodat afwijkingen sneller worden gedetecteerd.	9.1.2 12.4.1 12.4.2 12.4.3	Restrisico voor acceptatie	
R37	Activiteiten van systeembeheerders worden niet automatisch gecontroleerd. Ongeautoriseerde toegang (of handelingen) door een systeembeheerder blijft maximaal een maand	- Voor de meeste systemen is automatische controle van de logfiles al actief. - Van de CIMS systemen worden de logbestanden aangeleverd bij SIEM/SOC van RIVM, maar wordt nog handmatig de rapportage beoordeeld (de eerste maand wekelijk na live gang). - Na in productie name van CIMS zal	9.1.2 12.4.1 12.4.2 12.4.3	Restrisico voor acceptatie	

Samenvatting risico's vóór maatregelen

kans / impact	1 <1 keer per 10 jaar	2 Minimaal 1 keer per 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 hoog	R07	R05 R11 R12 R18 R20 R21 R22 R23 R24 R26 R27 R29 R30 R40	R01 R02 R03 R04 R06 R08 R09 R13 R14 R15 R17 R19 R25 R28	R38 R43 R44	R33 R35 R36 R37 R41 R42 R49
2 midden		R10 R16	R39 R45 R46	R34 R47 R48	
1 laag			R31 R32		

Samenvatting risico's na maatregelen

kans / impact	1 <1 keer per 10 jaar	2 Minimaal 1 keer per 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 hoog	R09 R13 R14 R15 R17 R44		R02 R08 R33 R36 R37		
2 midden		R16			
1 laag					

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*
Er zijn geen risico's geïdentificeerd die niet kunnen worden gemitigeerd. Het volledig oplossen van de restrisico's neemt echter meer tijd in beslag dan er rest voor de geplande releasedatum van CIMS (8 januari 2021).

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*
Niet van toepassing.

Periode *Geef aan voor welke periode de risicoacceptatie moet gaan gelden en wat de einddatum van deze acceptatie is*
Deze risicoacceptatie geldt vanaf livegang per 8 januari 2021 en is **geldig tot 1 oktober 2021.**

Evaluatie *Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden*
De vijf geïdentificeerde restrisico's worden opgenomen in het centrale risicoregister van RIVM CIO Office. De voortgang op het oplossen van de restrisico's wordt actief bewaakt en opgevolgd. Voor het verlopen van de acceptatieperiode wordt gecontroleerd of de risico's daadwerkelijk zijn opgelost en indien nodig geëscaleerd voor oplossing. Evaluatie wordt ondergebracht in een PDCA-cyclus.

Gevraagd besluit:	In te stemmen met genoemde beschrijving van het bestaan van een restrisico waarvan de kans van optreden wordt verkleind, maar dat continu onder de aandacht moet blijven.		
Partij	***Naam***	***Mening*** *(invullen door Hoofd centrum, IM, CISO, CIO, Privacy, DG, DR etc.)*	***Akkoord***
Hoofd centrum	5.1.2e		Akkoord: ja/nee
Domein IM	5.1.2e		Akkoord: ja/nee
CISO *(mandatory voor alle risk levels)*	5.1.2e	Akkoord met de inhoud en bij deze stem ik als CISO in met het gevraagde besluit hierop.	Akkoord: ja/~~nee~~
Compliance (Facultatief)	...		Akkoord: ja/nee
Legal (facultatief)	...		Akkoord: ja/nee
Privacy (facultatief)	...		Akkoord: ja/nee
CIO *(mandatory voor medium en hoger risico)*	5.1.2e		Akkoord: ja/nee
DR *(mandatory voor hoog en zeer hoog risico)*	5.1.2e / 5.1.2e		Akkoord: ja/nee