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

AANVRAAGFORMULIER RISICOACCEPTATIE

Betreft:	CIMS Rapportageomgeving
Aanvrager:	RIVM-DVP
Telefoonnummer:	
Aanvraagnummer:	20210222-01 RACC CIMS Rapportage
Datum aanvraag:	22-2-2021
Naam verantwoordelijk lijnmanager:	5.1.2e
Naam centrum- of afdelingshoofd:	5.1.2e
Centrum:	DVP
Naam Informatiemanager:	5.1.2e
Doel:	Vaststellen en beoordelen restrisico's
Aan:	5.1.2e (CISO RIVM)
T.b.v. vergadering:	Stuurgroep COVID-registratie
Aantal pagina's:	7
Document toegevoegd:	RIVM - Risicoanalyse CIMS-Rapportage v1.1 210222.xlsx
Versienummer	0.1
Datum laatst gewijzigd	22-2-2021

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										

Bovenstaande resultaat is gebaseerd op de Quickscan BIO voor CIMS 1.0

Aanvullende opmerkingen of randvoorwaarden

Security

- De risicoanalyse is uitgevoerd op basis van de situatie die is beschreven in 'PSA COVID Informatie Rapportage v0.90.docx' . Een definitieve versie (1.0) van de PSA moet nog worden vastgesteld.
- De wijze van **pseudonomisering** van data is uitgebreid besproken. De gekozen oplossing qua informatiebeveiliging akkoord bevonden.

Privacy

- Voor de CIMS Rapportageomgeving is geen aparte DPIA opgesteld; er is voor gekozen om een addendum te schrijven voor de DPIA op CIMS 1.0; hier is nog geen advies van de FG op ontvangen.
- De technische oplossing voor pseudonimisering is qua IB akkoord. De manier waarop deze oplossing ingezet wordt moet echter nog wel beoordeeld worden vanuit privacy-perspectief.
- Restrisico's die benoemd zijn in dit document, zijn niet meegenomen in het addendum op de DPIA.

Aanvraagnummer

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

20210222-01 RACC CIMS Rapportage

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.

De **CIMS-rapportageomgeving** heeft als doel een functie te realiseren die automatisch rapporten kan leveren voor de monitoring en evaluatie van het vaccinatieprogramma voor COVID-19. Dit betreft voornamelijk rapporten over de opkomst, vaccinatiegraad, effectiviteit en veiligheid. Maar gezien de noodzaak om kennis over de ziekte en vaccinaties te ontwikkelen zullen er daarnaast specifieke vragen komen die snel en flexibel beantwoord moeten kunnen worden.

Risicoanalyse

Er is een risicoanalyse uitgevoerd op basis van de systeemdecompositie, workshops, interviews en documentatiereviews (waaronder de Project Start Architectuur (PSA)). Een gedetailleerde blauwdruk van de omgeving was nog niet beschikbaar op moment van de uitgevoerde analyse, maar zal wel worden opgeleverd voor overdracht naar beheer. Er was wel voldoende informatie voorhanden om de systeemdecompositie op te stellen voor de analyse.

Rapportages zullen worden aangeleverd aan interne afnemers (EPI). Vanuit deze afnemers zullen rapportages eventueel gepubliceerd worden via de geijkte kanalen. Voor deze verdere verwerkingen zullen aparte analyses uitgevoerd worden m.b.t. privacy impact en waar nodig ook voor informatiebeveiligingsrisico's. Een penetratietest op de CIMS-rapportageomgeving is niet uitgevoerd; er is geen sprake van een koppeling met internet.

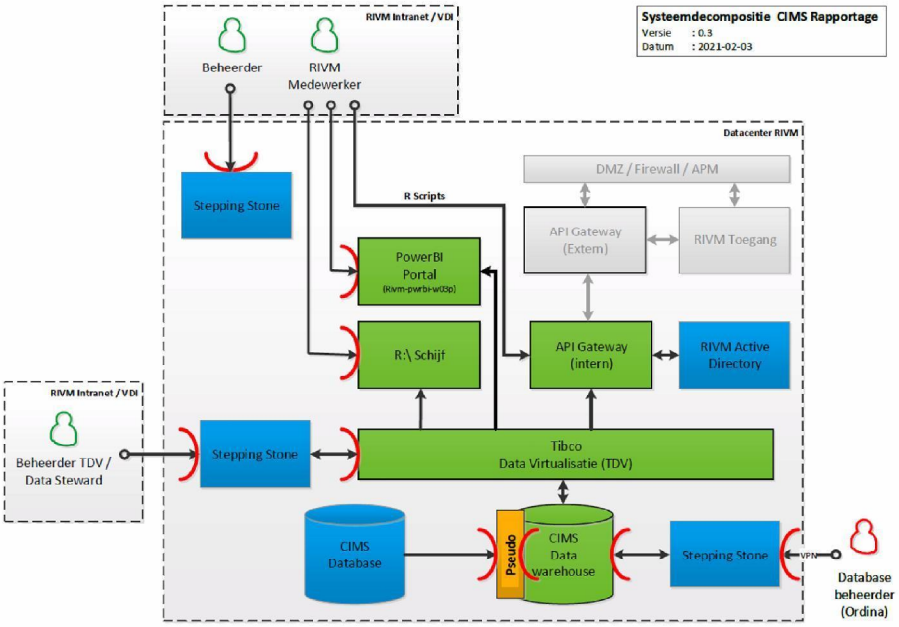
Er zijn 29 mogelijke risico's geïdentificeerd, waarvan er voor 22 al voldoende mitigerende maatregelen waren getroffen. Voor de 7 resterende mogelijke risico's zijn mitigerende maatregelen besproken waarvan er enkele nog door het projectteam kunnen worden geïmplementeerd om het totale restrisico te verlagen.

Advies

De 7 geïdentificeerde restrisico's voorlopig accepteren en de aanvullende maatregelen die worden genoemd in de risico-tabel op zeer korte termijn realiseren (voor 1 april).

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 waar mogelijk 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	Misbruik van onrechtmatig verkregen inloggegevens door een interne of externe aanvaller.	**Huidige maatregelen:** - Geen koppeling met internet - Twee-factor authenticatie - scheiding van rollen/rechten voor alle OTAP-omgevingen. - logging van activiteiten is actief (verhoogde dijkbewaking). **Nog te nemen maatregelen:** - Procesbeschrijving Identity & Access management (incl. rollen/rechten matrix), waarbij de beoordeling van aanvragen voor toegangsrechten ook onderdeel is van het proces. - Actieve monitoring van logfiles via SIEM/SOC regelen/bevestigen.	7.1.1 9.1 9.2 9.3 9.4 12.4 13.1 13.2 18.1	Restrisico voor acceptatie	
R18	Procesfouten vanwege het niet werken volgens voorschriften/procedures **door gebruikers**. Deze procesfouten zouden kunnen leiden tot ongeautoriseerde toegang tot rapportages.	**Huidige maatregelen:** De basisprocessen en procedures voor Praeventis/Praemis zijn al te gebruiken voor beheer en toegangsverlening. **Nog te nemen maatregelen:** - Specifieke processen/procedures voor Tibco Datavirtualisatie uitwerken, inclusief publicatieproces (via 'werkgroep gegevensverstrekking').	12.1 14.2	Restrisico voor acceptatie	
R20	Beheerfouten hebben schadelijke gevolgen voor de rapportageomgeving (bijv. uitvoeren van een schadelijk commando).	**Huidige maatregelen:** - Er wordt gewerkt via het 4-ogen principe door beheerders. - Strikte scheiding van OTAP-omgevingen. Publicatieproces dwingt het vier-ogen principe af. - Back-up is aanwezig. **Nog te nemen maatregelen:** - beschrijf de werking van het 4-ogen principe (eventueel als onderdeel van het IAM-proces).	12.1 12.3 14.2 14.3	Restrisico voor acceptatie	

R22	Procesfouten (onjuiste uitvoering van een procedure/richtlijn) **door beheerders**, waardoor het systeem foutief wordt geconfigureerd.	**Huidige maatregelen** - Basisprocessen en procedures voor Praeventis/Praemis zijn al te gebruiken. - Strikte scheiding tussen de O, T, A en P-omgevingen met aparte rollen/rechten. - Doorzetten van test -> acceptatie -> productie altijd via Change Management. - Logging van toegang/activiteiten is actief. - Autorisatiematrix is opgesteld voor TDV. **Nog te nemen maatregelen:** - Specifieke procedures opstellen voor beheerders TDV.	12.1 12.3 12.4 12.5 12.6 14.1 14.2 14.3	Restrisico voor acceptatie	
R27	Gegevens zijn onbedoeld te herleiden tot een persoon.	**Huidige maatregelen:** - Per veld kan pseudonimisering worden ingericht. - Techniek voor pseudonimisering is geselecteerd, gebouwd en beschreven. **Nog te nemen maatregelen:** - Geen aanvullende maatregelen nodig.	9.1 9.2 9.3 9.4 12.4 13.1	Restrisico voor acceptatie	
R28	Ongeautoriseerde toegang tot TDV en/of rapportages; de toegang is niet beperkt tot 'need to know'.	**Huidige maatregelen:** - Authenticatie en autorisatie in TDV is actief en gekoppeld aan RIVM Active Directory. - Logging staat aan. - Autorisatiematrix is opgesteld voor TDV **Nog te nemen maatregelen:** - beschrijven van identity & access managementproces voor rapportageomgeving CIMS.	9.1 9.2 9.3 9.4 12.4 13.1 18.1		
R29	Ontbrekende beveiligingsmaatregelen in het ontwerp van de CIMS-rapportage-omgeving.	**Huidige maatregelen:** - Concept Project Startarchitectuur (PSA) versie 0.90 is opgeleverd. **Nog te nemen maatregelen:** - Definitieve versie (1.0) van de PSA opleveren.	14.1 14.2 14.3		

Matrix - mogelijke 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		R02	R28 R29	R27	
2 midden		R18 R20 R22			
1 laag					

Matrix – restrisico's (na inmiddels genomen 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		R02 R27			
2 midden		R18 R20 R22 R28 R29			
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 op 25 februari.

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 25 februari 2021 en is **geldig tot 1 april 2021**.

Evaluatie *Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden*
De zeven 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 *(verplicht voor alle risk levels)*	5.1.2e		Akkoord: ja/nee
Compliance (Facultatief)	...		Akkoord: ja/nee
Legal (facultatief)	...		Akkoord: ja/nee
Privacy (facultatief)	...		Akkoord: ja/nee
CIO *(verplicht voor medium en hoger risico)*			Akkoord: ja/nee
DR *(verplicht voor hoog en zeer hoog risico)*			Akkoord: ja/nee