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:	20200902-01 RACC CIMS
Datum aanvraag:	25-09-2020
Naam verantwoordelijk lijnmanager:	
Naam centrum- of afdelingshoofd:	(10)(2e)
Centrum:	DVP
Naam Informatiemanager:	(10)(2e)
Doel:	Vaststellen risico's en te nemen maatregelen c.q. uit te stellen maatregelen
Aan:	...
T.b.v. vergadering:	...
Aantal pagina's:	...
Notitie toegevoegd:	...

Context / resultaat quickscan CVR

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:

- CIMS wordt gebouwd op een kopie van de Praeventis database.
- Praeventis heeft door privacy risico's/maatregelen doorlopen. De eisen t.a.v. CIMS zijn niet anders of hoger

dus dit voldoet voor CIMS. Wel maakt een PIA onderdeel uit van het te lopen ontwikkeltraject.

Aanvraagnummer

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

20200902-01 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, het doen van recalls en zicht houden op voorraden. Met registratie wordt de vastlegging van de vaccinatie bij een persoon bedoeld.

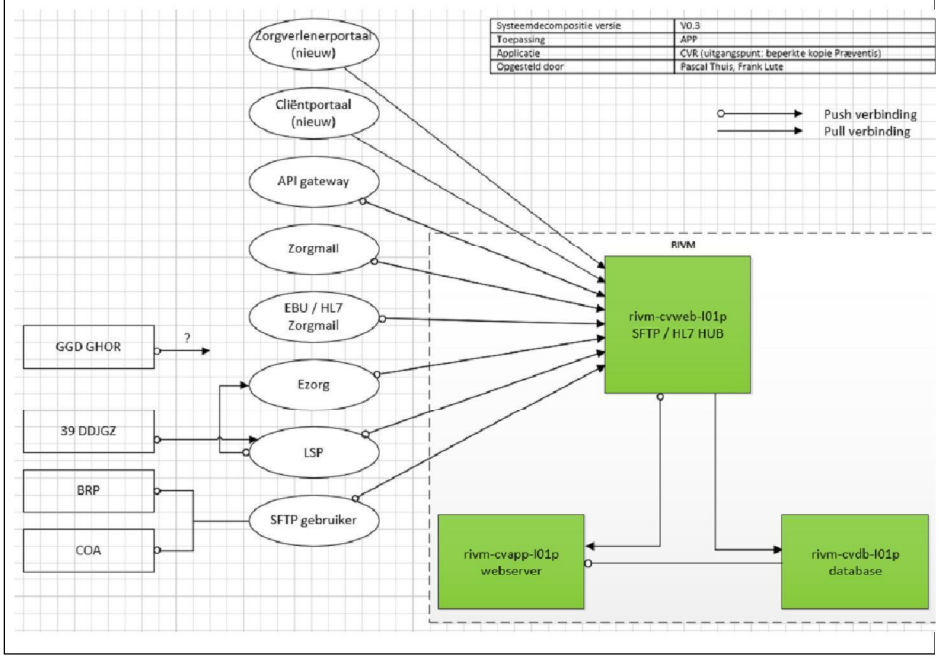
Het CIMS is gebouwd op een kopie van Praeventis. Praeventis verzorgt standaard de inkoop, opslag en registratie van vaccins en monitoring toediening vaccinaties. Behalve dat Praeventis de bovenstaande functies bevat, zijn ook de processen er omheen ingericht.

Het centrale registratiesysteem wordt gevoed vanuit bronsystemen van zorgverleners, en/of door directe handmatige data-invoer door zorgverleners. Dit laatste wordt mogelijk gemaakt door het ontwikkelen van een zorgverlenerportaal waar na beveiligde inlog (e-Herkenning) door zorgverlener de gevraagde gegevens kan insturen.

Er is een risicoanalyse uitgevoerd op basis van de uitgevoerde quickscan en systeemdecompositie.
In de risicoanalyse zijn initieel mogelijke risico's beschouwd. Hiervan zijn 32 risico's van toepassing verklaard op CIMS. Deze risico's zijn beoordeeld op kans en impact en 5 risico's hebben een kans midden of hoog. Deze 5 risico's kunnen alleen worden gemitigeerd met organisatorische maatregelen. In de risicoanalyse is een voorstel gedaan voor te treffen maatregelen.

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*			
		...			
Ref.	**Risico**	**Maatregel**	**Gerelateerde BIO norm** *Geef hier aan welk BIO-norm van toepassing is*	**Status** *(CISO RIVM)*	**Bijzonderheden** *(CISO RIVM)*
R01	Gebruik van de onrechtmatig verkregen inloggegevens van een medewerker of andere belanghebbende (brute-force aanval, phishing wachtwoord raden, onbeveiligde opslag van gegevens, gebruik van hetzelfde wachtwoord in meerdere, onafhankelijke omgevingen)	Security awareness	9.3.1 9.4.2.1		

R02	Misbruik van een kwetsbaarheid in het authenticatie en autorisatiemechanisme van een applicatie (bijvoorbeeld privilege escalation)	Netwerkzonering Pentest Geen single sign on	9.1.2		
R03	Session Hijacking (bijvoorbeeld session replay-aanvallen)	Strenge controle op de interfaces Pentest	9.4.1		
R04	Rechtstreeks misbruik van een kwetsbaarheid (ontbreken patch, misconfiguratie) in de infrastructuur (besturingssysteem, webserver, middleware, services, software)	Pentest Continue patchen	12.6.1		
R05	Denial-of-Service aanvallen (wireless jamming, distributed denial of service op een gateway)	Pentest vanaf internet op RIVM omgeving	13.1.2		
R06	Aanpassen van netwerkverkeer (bijvoorbeeld DNS-hijacking, Man-in-the-Middle)	Pentest	13.1.2		
R07	Afluisteren van netwerkverkeer (sniffen van onversleuteld of onvoldoende versleuteld netwerkverkeer)	Pentest Monitoren netwerkverkeer Alle gegevens versleutelen	13.1.2		
R08	Diefstal (lezen)/fraude/lekken van (gevoelige) gegevens	Security awareness	8.2.3		
R09	Fraude door de invoer van valse transacties	Controle op de rapportages Correctieberichten Automatiseren van gegevensinvoer	12.2.1		
R10	Valsheid in geschrifte	Veilig inloggen uitvoerende instanties (minimaal 2-factor).	12.2.1 9.4.2		
R11	Aanpassing van gegevens, manipulatie van programmatuur voor na ingebruikname	Geheimhoudingsverklaring Integriteitsverklaring	12.2.1		
R12	Vernietigen van gegevens	Alleen functioneel- en technisch beheerders kunnen gegevens verwijderen	12.2.1 9.4.2		
R13	Installatie malware met als doel gegevens te vernietigen	Medewerkers mogen alleen de Campus Pro werkplek gebruiken. Bij Campus VDI is applicatie whitelisting. Alleen op de uitwijk PC's regelen.	12.2.1		
R14	Installatie malware met als doel gegevens te lekken	Medewerkers mogen alleen de Campus Pro werkplek gebruiken. Bij Campus VDI is applicatie whitelisting. Alleen op de uitwijk PC's regelen.	12.2.1		

R15	Installatie malware met als doel een externe aanvaller toegang tot de omgeving te verschaffen	Medewerkers mogen alleen de Campus Pro werkplek gebruiken. Bij Campus VDI is applicatie whitelisting. Alleen op de uitwijk PC's regelen.	12.2.1		
R16	Installatie malware met als doel om gegevens te versleutelen en een aanvaller in staat te stellen "losgeld" te vragen	Medewerkers mogen alleen de Campus Pro werkplek gebruiken. Bij Campus VDI is applicatie whitelisting. Alleen op de uitwijk PC's regelen.	12.2.1		
R17	Phishing (phishing, spear-phishing, whaling)	Verkeerde linkjes afhouden in de mail. Security awareness. Integriteitsverklaring.	7.2.2 9.4.2 13.2.3		
R18	Installatie van spyware via toegang hardware (spyware) op locatie RIVM of in fabriek	Alleen op de uitwijk PC's regelen. Deze volledig dichtzetten.	12.2.1		
R19	Afpersing van individuen om informatie beschikbaar te stellen of om bepaalde activiteiten uit te voeren (gijzeling, charge) door verbaal of fysiek agressief/gewelddadig gedrag.	Security awareness Ondersteuning RIVM bij incidenten	7.2.2 11.1.4		
R20	Afluisteren aftappen van netwerkverkeer	Pentest Monitoren netwerkverkeer Alle gegevens versleutelen	13.1.2		
R21	Procesfouten (het niet juist uitvoeren van procedures, het nalaten van de uitvoering van vereiste acties, en gebrek aan zorgvuldigheid en zelfcontrole bij de uitvoering van acties), Niet werken volgens voorschriften/procedures (gebrek motivatie/loyaliteit)	Scheiding van OTAP straten. Scheiding van netwerkzones. Of anders voorschriften/ procedures.	9.1.2 13.1.3		
R22	Verlies van wachtwoordgegevens en andere informatie die misbruikt kan worden (op papier, op gegevensdragers zoals USB-sticks)) **door medewerker**	Security awareness	8.2.3 8.3.3 9.1.1 9.1.2		
R23	Beheerfouten (bijvoorbeeld uitvoeren commando met high-privileged account met schadelijke gevolgen)	Voor functioneel- en technisch beheerders extra checks en logging. Is er een goede backup?	9.4.2.1 9.4.4.1 9.4.4.2 12.1.1		
R24	Installatie van malware of software met malware ingebouwd	Navragen (10)(2e)	12.2.1 12.5.1		

R25	Procesfouten (onjuiste uitvoering van een procedure/richtlijnen, waardoor bijvoorbeeld een systeem foutief wordt geconfigureerd, een softwarewijziging onjuist wordt geïmplementeerd en dergelijke) Niet werken volgens voorschriften/procedures (gebrek motivatie/loyaliteit).	Ontwikkelaars alleen tijdelijk toegang geven tot de productieomgeving voor hulp bij productieverstoringen. Voorschriften/procedures maken voor testen in de acceptatieomgeving.	9.2.2 9.2.3		
R26	Verlies van wachtwoordgegevens en andere informatie die misbruikt kan worden (op papier, op gegevensdragers zoals USB-sticks) **door IT-medewerker**	Security awareness	8.2.3 8.3.3 9.1.1 9.1.2 12.1.1		
R27	Ongeautoriseerd mutaties doorvoeren (afstand overnemen van systeem)	Veilig inloggen leverancier (minimaal 2-factor).	9.4.4		
R28	Misconfiguratie van een systeem of beveiligde verbinding, waardoor een kwetsbaarheid met gevolgen voor de beveiliging van de ICT-omgeving van RIVM ontstaat (ketenpartner wordt 'stepping stone')	Regelmatige pentest	9.1.2		
R29	Foutieve verwerking door software (en niet testen)	*Pentesten*	12.1.4		
R30	Achterdeur in de programmatuur	*Pentesten*	12.1.4		
R31	Ziektegolf door besmetting met virus of bacterie	Thuiswerken Vervanging van medewerkers door collega's/ketenpartners	7.2.1		
R32	Voedselvergiftiging	Thuiswerken Vervanging van medewerkers door collega's/ketenpartners	7.2.1		

Samenvatting risico's vóór maatregelen

impact \ kans	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 R03 R05 R26	R01 R04 R06 R07 R08 R11 R12 R13 R14 R15 R16 R17 R18 R20 R21 R22 R23 R24 R27 R28 R29 R30	R09 R19 R25 R31 R32		
2 midden					
1 laag		R10			

Samenvatting risico's na maatregelen

impact \ kans	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 R03 R05 R26	R01 R04 R06 R07 R08 R09 R11 R12 R13 R14 R15 R16 R17 R18 R19 R20 R21 R22 R23 R24 R25 R27 R28 R29 R30 R31 R32			
2 midden					
1 laag		R10			

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*
In principe komen uit de risicoanalyse CIMS geen maatregelen naar voren die niet kunnen worden uitgevoerd. De genoemde maatregelen zijn organisatorisch van aard, te weten het vergroten van security awareness bij uitvoerenden DVP en het uitvoeren van een pentest. Deze maatregelen zullen het risico zeker verkleinen maar moeten elk jaar opnieuw onder aandacht worden gebracht. Het risico blijft namelijk altijd bestaan. Vandaar dat ze in deze risicoacceptatie worden opgenomen.

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*
De genoemde risico's die blijven bestaan ondanks de uit te voeren maatregelen hebben direct invloed op zorgverleners, betrokkenen (volgens AVG-definitie), uitvoerders DVP en overige ketenpartners.

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 15 december 2020 en is geldig tot 1 oktober 2021.

Evaluatie *Geef aan wanneer en op welke wijze evaluatie van het restrisico zal gaan plaatsvinden*
De restrisico's betreffen: • R09 - Fraude door de invoer van valse transacties. Hiertoe worden controles uitgevoerd op de rapportages, worden correctieberichten verstuurd en wordt gegevensinvoer geautomatiseerd. • R19 - Afpersing van individuen om informatie beschikbaar te stellen of om bepaalde activiteiten uit te voeren (gijzeling, charge) door verbaal of fysiek agressief/gewelddadig gedrag. Hiertoe worden security awareness trainingen gegeven en wordt ondersteuning gegevens bij incidenten. • R25 - Procesfouten (onjuiste uitvoering van een procedure/richtlijnen, waardoor bijvoorbeeld een systeem foutief wordt geconfigureerd, een softwarewijziging onjuist wordt geïmplementeerd en dergelijke) Niet werken volgens voorschriften/procedures (gebrek motivatie/loyaliteit). Hiertoe worden ontwikkelaars alleen tijdelijk toegang gegeven tot de productieomgeving voor hulp bij productieverstoringen. En worden voorschriften/procedures gemaakt voor testen in de acceptatieomgeving. • R31 - Ziektegolf door besmetting met virus of bacterie. Hiertoe wordt thuiswerken bevorderd en wordt vervanging geregeld van medewerkers door collega's/ketenpartners. • R32 – Voedselvergiftiging. Hiertoe wordt thuiswerken bevorderd en wordt vervanging geregeld van medewerkers door collega's/ketenpartners. Door organisatorische maatregelen wordt de kans op het optreden van deze risico's verkleind. De maatregelen worden ieder jaar opnieuw onder aandacht gebracht maar als de maatregelen niet goed werken blijven de risico's dusdanig groot dat deze geaccepteerd moeten worden. 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	(10)(2e) a.i.		Akkoord: ja/nee
Domein IM	(10)(2e)		Akkoord: ja/nee
CISO *(mandatory voor alle risk levels)*	(10)(2e)		Akkoord: ja/nee

Compliance (Facultatief)	...		Akkoord: ja/nee
Legal (facultatief)	...		Akkoord: ja/nee
Privacy (facultatief)	(10)(2e)		Akkoord: ja/nee
CIO *(mandatory voor medium en hoger risico)*	(10)(2e)		Akkoord: ja/nee
DR *(mandatory voor hoog en zeer hoog risico)*	...		Akkoord: ja/nee