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

Stuurgroep Registratie COVID vaccinatie programma

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl

KvK Utrecht 30276683

5.1.2e

memo

Oplegnotitie Risicoregister CIMS

Datum
6 januari 2021

Ons kenmerk
DPV_205

Behandeld door
5.1.2e
5.1.2e
5.1.2e 5.1.2e rivm.nl

Beste leden van de stuurgroep,

Gevraagd besluit:
De stuurgroep wordt gevraagd om:

(1) Akkoord te gaan met het accepteren van de 5 informatiebeveiligings(rest)risico's zoals deze benoemd zijn voor live gang bij de eerste release van COVID Informatie Monitoring Systeem (CIMS);
(2) De beschreven vervolgacties voor ná live gang te accorderen;
(3) En de conclusie te ondersteunen dat er geen belemmeringen zijn, vanuit informatiebeveiliging, die een live gang van de eerste release van CIMS op uiterlijk 8 januari in de weg staan.

Attentiepunten: er is een cross check uitgevoerd op de Data Protection Impact Assessment (dPIA) van de eerste release van CIMS, omdat informatiebeveiligingsrisico's van invloed zijn op de privacy risico's en vice versa. De dPIA zal apart door de Stuurgroep worden geaccordeerd.

Zie hieronder de samenvatting Analyse informatiebeveiligingsrisico CIMS eerste release met betreffende bijlagen CIMS_Issue_actielijst P_IB vs 1.8 (in deze bijlage zijn ook vervolgacties opgenomen voor ná live gang) en het standaard aanvraagformulier risicoacceptatie ter ondertekening (DPV_131 Aanvraagformulier risicoacceptatie CIMS v1.0).

Analyse informatiebeveiligingsrisico's CIMS eerste release

Conclusie en advies: accepteer de informatiebeveiligings(rest)risico's voor live gang van de eerste release van CIMS

Met een zorgvuldige aanpak zijn de informatiebeveiligings(rest)risico's voor deze scope inzichtelijk gemaakt en vastgelegd. Acties en mitigerende maatregelen voor de (rest)risico's zijn voortvarend aangepakt. Het overal risicobeeld is laag. Vervolgacties voor ná live gang worden verder opgepakt.

Acties en mitigerende maatregelen voor 5 (rest)risico's met kwalificatie midden (oranje) zijn niet (geheel) afgerond of worden niet opgelost voor live gang 8 januari as.

Ref.	Omschrijving	Risico	Mitigerende maatregelen aanwezig
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.
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
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.
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.

R37	Activiteiten van systeembeheerders worden niet automatisch gecontroleerd.	Ongeautoriseerde toegang (of handelingen) door een systeembeheerder blijft maximaal een maand onopgemerkt.	- 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 monitoring worden geautomatiseerd uiterlijk na een maand van live gang zodat afwijkingen nog sneller worden gedetecteerd.

Achtergrond
De afgelopen weken is bij het RIVM een eerste inventarisatie gemaakt van de informatiebeveiligingsrisico's (conform ISO 27005 norm) voor het inrichten van een landelijk registratiesysteem voor de COVID-vaccinatie.

Doel en scope
Het doel van deze inventarisatie is om de informatiebeveiligingsrisico's vóór de live gang van de eerste release van CIMS inzichtelijk te maken, daarop acties in te plannen c.q. af te ronden en ervoor te zorgen dat een weloverwogen besluit voor live gang genomen kan worden door de Stuurgroep Registratie van het COVID-vaccinatie programma van het RIVM.

De scope betreft het proces vanaf het ontvangen van vaccinatie data en het registreren daarvan in het COVID Informatie en Monitoring Systeem (CIMS). Dit proces wordt ondersteund door de CIMS-applicatie (eerste release), een Secure File Transfer Protocol (SFTP) server en een daarvoor ingericht technische infrastructuur, incl. een database van Oracle.

Voor ingebruikname van de overige componenten van het project (cliëntenportaal, zorgverlenersportaal (tijdelijke gestopt), API Gateway en datawarehouse BI-CIMS), worden nog separaat analyses uitgevoerd voor live gang. Overigens zo ook voor RIVMToegang en bestelmodule, die buiten de scope van het project CIMS vallen.

De inventarisatie van de informatiebeveiligings(rest)risico's is gebaseerd op analyses gedaan door het RIVM zelf, aandachtspunten meegegeven door National Cyber Security Center (NCSC), aanbevelingen van VWS ([redacted] en rapportages van externe partijen Secura, Noordbeek en de ADR.

Risicoanalyses voor de GGDGHOR, Acute Zorg en BRBA zijn hierbij niet meegenomen.

Door het adresseren van informatiebeveiligingsrisico's worden ook voor een groot deel de risico's op het gebied van privacy aangepakt. Deze zijn opgenomen in de betreffende dPIA.

Aanpak zorgvuldig
Deze risico-inventarisatie is gebaseerd op de risicoanalyses van het RIVM. Hiervoor zijn workshops "risicoanalyse" gehouden en documenten geraadpleegd zoals risico-inventarisatie Basis Infrastructuur, penetratie test Praeventis en bijbehorende technische documentatie van CIMS.

De aanbevelingen van VWS ([redacted] zijn geadresseerd, aandachtspunten genoemd door het NCSC zijn doorgesproken, de bevindingen van de onderzoeken door Secura, Noordbeek en de ADR zijn opgepakt.

De analyses zijn uitgevoerd door een team bestaande uit medewerkers van het project CIMS, DVP Beheer, IV Basis Infrastructuur, Informatiebeveiliging en Informatiemanagement. Voor de (zeer)hoge risico's is ook advies verkregen van Ordina en zijn deze verwerkt. Het NCSC heeft meegekeken.

Per risico (of groep van risico's) zijn de daarop betrekking hebbende Baseline Informatiebeveiliging Overheid (BIO) richtlijnen vermeld en mogelijk impact op privacy. De score die per risico is aangegeven is relatief hoger door het hoger vereiste veiligheidsniveau.

Voor het kwalificeren van de risico's zijn kleuren toegekend conform de methode risicoanalyse BIO, waarbij rood aangeeft een (zeer)hoog risico, oranje en geel een middel risico aangeven en groen een (zeer)laag risico.

Risico's die niet per 1-8-2021 gemitigeerd worden zullen op een 'roadmap' worden geplaatst en in het "driehoek" overleg tussen Beheer (DVP) Basis Infrastructuur en Ordina (technisch applicatie beheer) worden bewaakt en opgelost.

De risico's aangegeven door de externe partijen Secura en ADR kennen de kwalificaties hoog, midden, laag. Het rapport Noordbeek geeft aanbevelingen die door het RIVM Informatiebeveiliging zijn vertaald naar de kwalificaties hoog, midden, laag.

Analyse van informatiebeveiligingsrisico's

Informatiebeveiligingsrisico's voortvarend aangepakt en risicobeeld is nu laag

De afgelopen weken zijn veel mitigerende maatregelen en acties afgerond, waardoor de bijbehorende risico's een lagere risico kwalificatie hebben gekregen en of opgelost zijn vóór live gang.

Bij een vergelijk tussen het risicobeeld aan het begin van de analyse en nu (zie de twee matrices hieronder) is goed te zien dat het overall risicobeeld voor deze live gang teruggebracht is naar de kwalificatie laag als het gaat om de door RIVM uitgevoerde risicoanalyse.

Risicomatrix IB Risicoanalyse – originele analyse

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		

Risicomatrix IB Risicoanalyse – na genomen maatregelen

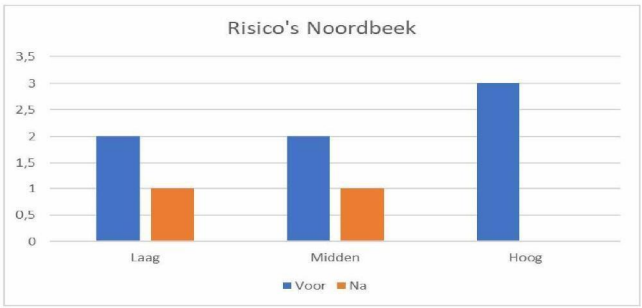
kans / impact	1 <1 keer per 10 jaar	2 Minimaal 1 keer per 5 jaar	3 Minimaal 1 keer per jaar	4 Elk kwartaal	5 Een keer per maand of vaker
3 hoog	R09 R13 R14 R15 R17 R44		R02 R08 R33 R36 R37		
2 midden		R16			
1 laag					

Restrisico's die gereed zijn en of opgelost zijn komen niet meer voor in deze matrix.

Zoals hierboven aangegeven blijven er nog 5 restrisico's over die niet (geheel) gereed zijn of opgelost worden voor live gang, uiterlijk 8 januari 2021.

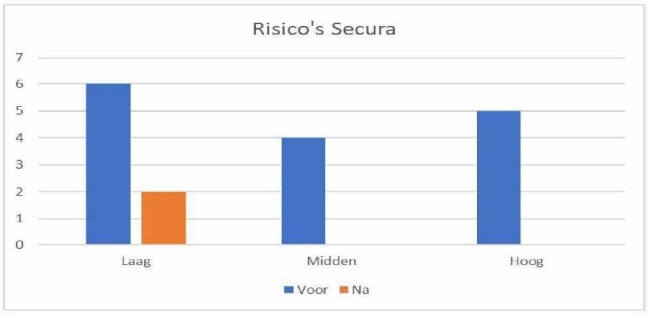
Ook het risicobeeld op basis van de door derde partijen uitgevoerde onderzoeken laat zien dat dit per 8 januari laag is.

Risico's Noordbeek:

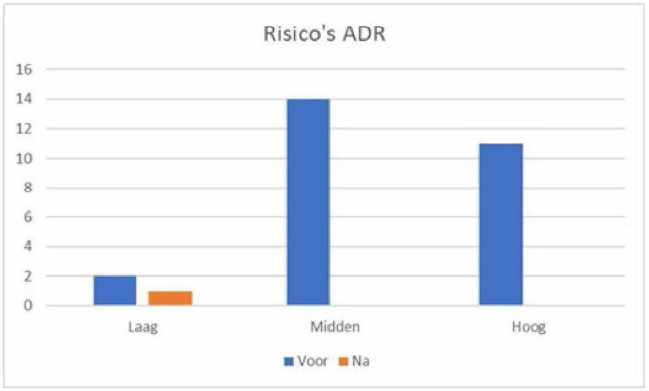


In dit overzicht zijn de bevindingen van Noordbeek door RIVM vertaald naar een categorie laag, midden of hoog. Oranje (midden) is het restrisico betreffende het CSV bestand (R08).

Risico's Secura:



Risico's ADR



Vervolgacties voor ná live gang

Uit deze risicoanalyse zijn de eerstvolgende acties geformuleerd voor ná live gang. Het voeren van de regie, het rapporteren over en het bewaken van de voortgang van deze acties ligt vooralsnog bij de programma regisseur CIMS van de IV organisatie in nauwe samenwerking met het programma team CIMS.

Item#	Wat	Wie	Wanneer
1	Opstellen audit kalender (pentesten, Quick Scans, toetsen, dPIA, IB, audits, etc.)	5.1.2e	Week 2-3
2	Uitvoeren toets op de werking van CIMS release 1.0	5.1.2e	Eind januari start
3	Inregelen voortgangsoverleg (wekelijks)	5.1.2e	Week 1

4	Bepalen nieuwe opzet risicoanalyse met NCSC	5.1.2e	Week 2
5	Verder op orde brengen documentatie CIMS	5.1.2e	Continu
6	Documenteren eigenaarschap CIMS	5.1.2e	Week 2
7	Opnemen vervolgacties in 'roadmap' met "driehoek"	5.1.2e	Week 1