Noordbeek

Rijndijk 235
2394 CD Hazerswoude
Tel. (071) 3416911
5.1.5 @noordbeek.com

Rijksinstituut voor Volksgezondheid en Milieu (RIVM)

ISAE 4401 Rapport van feitelijke bevindingen over Informatiebeveiliging

Aangaande een quick scan op het 'COVID-vaccinatie Informatie- en Monitoringsysteem' (CIMS)

Voor compliance met de BIO

Definitieve versie: 1.00

Opdrachtgever		RIVM
Auteurs	5.1.2e	Noordbeek B.V.
Rapportnummer	RIVQSC0-1	
Classificatie	Openbaar	
Status	Definitief	
Datum	8 januari 2021	
Bestandsnaam	Noordbeek Rapport RIVM Quick Scan BIO op CIMS	
KvK nummer	33265070	
BTW nummer	NL8203.45.180.B01	

Colofon

Opdrachtgever	5.1.2e
Opdrachtnemer	5.1.2e Email 5.1.2e @noordbeek.com
Contactpersoon	5.1.2e Email 5.1.2e @noordbeek.com
Auteur	5.1.2e
Kwaliteitscontrole	5.1.2e

Inhoud

1. Management samenvatting 4
1.1. Hoofdconclusie 4
1.2. Conclusie over risicobeheersing 4
1.3. Conclusie over compliance met de BIO 5
1.4. Conclusie over het Basisbeveiligingsniveau (BBN) 5
1.5. Conclusie over datacommunicatie 6
1.6. Conclusie over de keten 6

2. Rapport van feitelijke bevindingen met betrekking tot de quick scan 7
2.1. Opdracht 7
2.2. Verantwoordelijkheden 7
2.3. Werkzaamheden en bevindingen 8
2.4. Overzicht van de adviezen 9
2.5. Vrij gebruik van het rapport en de verspreidingskring 10

3. Detailrapport: Waarnemingen en conclusies per aandachtsgebied 11
3.1. Informatie binnen CIMS 11
3.2. Risicobeheersing voor CIMS 12
3.3. Logische toegangsbeveiliging 13
3.4. Fysieke toegangsbeveiliging 14
3.5. Communicatiebeveiliging 14
3.5.1. Uitwisseling van gegevens via csv-bestanden 14
3.5.2. Uitwisseling van vaccinatiegegevens met GGD GHOR 15

Bijlage A Overzicht van gesprekken en waarneming 16

Bijlage B Lijst van geraadpleegde documentatie 17

Bijlage C Lijst van afkortingen 18

1. Management samenvatting

Het RIVM ontwikkelt het 'COVID-vaccinatie Informatie- en Monitoringsysteem' (CIMS). Het RIVM heeft, in overleg met het ministerie van VWS, Noordbeek opdracht gegeven een quick scan uit te voeren op de beheersingsmaatregelen binnen de CIMS-omgeving, gericht op informatiebeveiliging conform de 'Baseline Informatiebeveiliging Overheid' (BIO).

Dit is aangevuld met een toetsing tegen het 'Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie' (VIR-BI) op het niveau 'Departementaal Vertrouwelijk' (DV).

Wij hebben geen onderzoek gedaan naar technische instellingen en patch-niveaus.

1.1. Hoofdconclusie

Tijdens onze quick scan hebben wij geen materiële afwijkingen geconstateerd ten opzichte van de BIO, die een inproductiename van CIMS Release 1 in de weg staan.

Wij adviseren het RIVM doorlopend aandacht te besteden aan de nog openstaande actiepunten in relatie tot de BIO, conform de adviezen in dit rapport en de reeds door het RIVM zelf in kaart gebrachte lopende verbeteracties.

Wij schatten het risico van het optreden van een materieel informatiebeveiligingsincident tijdens de productiefase van CIMS release 1 in als 'laag' tot 'gemiddeld', gezien de al getroffen beveiligingsmaatregelen, de lopende verbeteracties en de beperking van de toegang tot alleen geautoriseerde RIVM-medewerkers.

Wij willen complimenten uitspreken voor de medewerkers van het RIVM die betrokken zijn bij de ontwikkeling van CIMS, gezien de vele activiteiten die recentelijk zijn uitgevoerd voor risicobeheersing en het treffen van beveiligingsmaatregelen.

1.2. Conclusie over risicobeheersing

Naar onze mening heeft het RIVM op een adequate wijze risicobeheersing opgezet voor de CIMS-omgeving.

Wij hebben diverse actuele spreadsheets en documenten ontvangen, waaruit blijkt dat diverse bronnen zijn benut voor het inventariseren van de dreigingen en waarin de nog te treffen beveiligingsmaatregelen zijn beschreven, evenals de voortgang van hun implementatie. De risico's zijn ingeschat op basis van hun kans van optreden en impact, gerelateerd aan actuele dreigende actoren en situaties.

Naar onze mening heeft het RIVM bij haar risicobeheersing voldoende aandacht besteed aan alle doelstellingen van de BIO, met betrekking tot de CIMS-omgeving.

1.3. Conclusie over compliance met de BIO

Er is een aantal afwijkingen ten opzichte van de BIO, die door het RIVM zelf al in kaart zijn gebracht.

Deze afwijkingen hebben onder andere betrekking op ontbrekende of niet actuele documentatie, een nog lopende inventarisatie van toegangsbevoegdheden, incomplete logging en monitoring en de nog in te richten back-up-omgeving.

Een belangrijk issue is de tijdsdruk van het project en de soms veranderende uitgangspunten, waardoor de focus van het ontwerpteam primair ligt op het behalen van de deadline voor veilige productie. Hierbij worden de geprioriteerde beveiligingsmaatregelen meegenomen, maar komen documentatie en de minder urgente beveiligingsmaatregelen pas in een later stadium.

Wij hebben een kanttekening bij de voorgenomen inrichting van de back-up-omgeving. Gezien de recente ransomware-aanvallen op de overheid adviseren wij naast on-line back-up tevens een periodieke off-line back-up in te richten met verschillende retentieperiodes. Bij een juiste inrichting van de aanvullende off-line back-up is CIMS op een robuustere wijze bestand tegen ransomware.

1.4. Conclusie over het Basisbeveiligingsniveau (BBN)

Het reguliere Basisbeveiligingsniveau is 2 (BBN2) voor gegevensverwerking binnen de overheid.

Gezien de (geo)politieke gevoeligheid van het vaccinatieprogramma hebben wij CIMS tevens getoetst aan de eisen voor Basisbeveiligingsniveau 3 (BBN3), conform het 'Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie' (VIR-BI) op het niveau 'Departementaal Vertrouwelijk' (DV). Hierbij hebben wij vier aspecten uit het VIR-BI beschouwd, namelijk:

1. **Eigenaarschap**
   Wij hebben geen afwijkingen geconstateerd voor de inrichting van het eigenaarschap in relatie tot het VIR-BI. Het eigenaarschap lijkt op het niveau BBN3 te liggen, maar dit kan niet formeel worden vastgesteld aangezien het eigenaarschap niet is gedocumenteerd conform het VIR-BI;

2. **Fysieke toegangsbeveiliging van het datacenter**
   Wij hebben de CIMS-omgeving in het datacenter bezocht en visueel geïnspecteerd. Hierbij hebben wij geen afwijkingen geconstateerd voor de fysieke beveiligingsmaatregelen, conform het VIR-BI. Aangezien dit gedeelte van het datacenter regelmatig wordt geaudit namens de bevoegde instanties, kunnen de fysieke beveiligingsmaatregelen voor de CIMS-omgeving worden gezien als BBN3;

3. **Logische toegangsbeveiliging van de CIMS-omgeving**
   De rollen en bevoegdheden binnen CIMS zijn deels gekopieerd vanuit het Praeventis-systeem. Er lopen nog acties voor het inventariseren en inrichten van het accountbeheer. Het proces is slechts deels beschreven, aan de VIR-BI-eis 'minste privilege' is niet voldaan en

monitoring via SIEM/SOC moet nog worden ingericht. Op dit moment ligt het stelsel van maatregelen voor logische toegangsbeveiliging op het niveau BBN2;

4. **De levenscyclus van de CIMS-omgeving**
   Het RIVM heeft risicobeheersing adequaat ingericht en laat periodiek audits uitvoeren, waarbij de intentie is dit ook te doen voor de CIMS-omgeving. In dit kader lijkt de levenscyclus op het niveau BBN3 te liggen, maar dit kan niet formeel worden vastgesteld aangezien de levenscyclus niet is gedocumenteerd conform het VIR-BI.

1.5. Conclusie over datacommunicatie

De meeste communicatieverbindingen met de CIMS-omgeving zijn volgens de geïnterviewden voorzien van veilige protocollen en mechanieken.

Een uitzondering hierop vormt de server voor het Secure File Transfer Protocol (SFTP) en de mailbox voor E-Zorg. De SFTP-server en mailbox worden gebruikt voor het transport van bestanden met het formaat Comma Separated Value (csv) van en naar ketenpartners. In principe is het mogelijk dat deze bestanden ergens in de keten op een ongeautoriseerde wijze worden gekopieerd of worden gemanipuleerd.

Het RIVM is bezig een Gateway in te richten voor Application Programming Interface (API), waarbij de informatieuitwisseling op een veilige manier kan plaatsvinden. Niettemin vereist het gebruik van de API Gateway technische aanpassingen bij ketenpartners. Het blijkt dat niet alle ketenpartners in staat zijn gebruik te maken van deze veilige wijze van informatieuitwisseling.

Wij adviseren technische maatregelen te treffen om de vertrouwelijkheid en integriteit van csv-bestanden te borgen binnen de keten, in samenwerking met de ketenpartners.

1.6. Conclusie over de keten

De CIMS-omgeving bevat alleen de centrale registratie van het vaccinatieprogramma, gericht op centrale bewaking en monitoring. De registratie is beperkt tot de informatie waarvoor de betreffende burger heeft ingestemd via Informed Consent.

Wij hebben geen assurance dat voor andere systemen binnen de keten eenzelfde niveau van informatiebeveiliging is geborgd als voor de CIMS-omgeving.

Voor CIMS release 1 hebben wij vernomen dat het systeem CoronIT van GGD GHOR wordt aangesloten via een ODBC-koppeling op een Postgress-afslag van de database van CoronIT [doc 45].

Wij adviseren quick scans uit te laten voeren op compliance met de BIO voor de belangrijkste systemen binnen de keten, te starten met CoronIT en de ODBC-koppeling met CIMS.

2. Rapport van feitelijke bevindingen met betrekking tot de quick scan

Aan: Opdrachtgever

2.1. Opdracht

Wij hebben overeengekomen specifieke werkzaamheden verricht met betrekking tot een quick scan op de beheersingsmaatregelen binnen de CIMS-omgeving, gericht op informatiebeveiliging.

De opdracht voor de quick scan is overeengekomen met het RIVM en heeft als doel een beperkte mate van zekerheid te bieden dat de vereiste beheersingsmaatregelen in opzet en bestaan aanwezig zijn, en eventuele afwijkingen te beschrijven. Hierbij worden de getroffen beheersingsmaatregelen getoetst tegen 'Baseline Informatiebeveiliging Overheid' (BIO), die overeenkomt met de internationale standaard ISO/IEC 27001:2013 'Information Security Management Systems – Requirements'.

Een quick scan levert een beperkte mate van zekerheid, en is gericht op specifieke vragen die zijn geformuleerd door de opdrachtgever. Noordbeek levert de rapportage in de vorm van de 'International Standard on Assurance Engagements 4401' (ISAE 4401), met de Nederlandstalige naam 'Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden'.

De overeengekomen specifieke werkzaamheden zijn tot stand gekomen in overleg met de beoogde gebruikers, zijnde het RIVM en het ministerie van VWS.

De opdrachtvoorwaarden zijn omschreven in onze opdrachtbrief van 24 december 2020, uitgebracht door Noordbeek B.V.

De opdracht aan Noordbeek is onderdeel van een reeks aan onderzoeken en audits op het vaccinatieprogramma voor COVID-19, gericht op transparantie naar de burger en de volksvertegenwoordiging. In dit kader is dit ISAE 4401-rapport bedoeld om publiekelijk te worden gedeeld.

2.2. Verantwoordelijkheden

Het is de verantwoordelijkheid van het RIVM om te bepalen of de overeengekomen specifieke werkzaamheden toereikend en geschikt zijn voor het hierboven beschreven doel.

Wij hebben onze werkzaamheden verricht in overeenstemming met de Nederlandse Standaard 4401 'Opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden' van de Nederlandse Orde van Register IT-Auditors (NOREA).

Bij het uitvoeren van deze opdracht hebben wij ons gehouden aan de voor ons geldende relevante ethische voorschriften in de 'Verordening Gedrags- en Beroepsregels Accountants' (VGBA). Verder hebben wij de onafhankelijkheidsregels van de 'Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten' (ViO) in acht genomen.

2.3. *Werkzaamheden en bevindingen*

In aanvulling op de uitleg van de randvoorwaarden van de opdracht, zoals vermeld in de paragraaf 'Opdracht' is in deze paragraaf een beschrijving van de overeengekomen specifieke werkzaamheden en feitelijke bevindingen opgenomen.

Wij doen geen uitspraak over wat de feitelijke bevindingen betekenen voor informatiebeveiliging binnen de CIMS-omgeving in zijn totaliteit. Het RIVM en het ministerie van VWS zullen hierover een eigen afweging moeten maken, waarbij het RIVM en het ministerie van VWS gebruik kunnen maken van dit rapport van feitelijke bevindingen en eventuele andere beschikbare informatie.

Conform de opdracht in de offerteaanvraag zijn wij bij deze quick scan nagegaan of er een beperkte mate van zekerheid kan worden verkregen met betrekking tot de volgende punten:

1. Verifieer of de relevante beveiligingsmaatregelen in de CIMS-omgeving zijn gerealiseerd of gepland, conform de 'Baseline Informatiebeveiliging Overheid' (BIO);
2. Verifieer of de getroffen beveiligingsmaatregelen een Basisbeveiligingsniveau 2 (BBN2) borgen voor reguliere gegevensverwerking binnen de overheid, of al een Basisbeveiligingsniveau 3 (BBN3) mogelijk maken conform het 'Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie' (VIR-BI) op het niveau 'Departementaal Vertrouwelijk' (DV);
3. Verifieer of het RIVM risicobeheersing heeft ingericht voor de CIMS-omgeving, en of het RIVM daarmee een volledig zicht heeft op de nog openstaande acties die zijn vereist voor compliance met de BIO.

In overeenstemming met de opdrachtvoorwaarden zijn wij nagegaan of:

- De vereiste beheersingsmaatregelen voor informatiebeveiliging in de CIMS-omgeving van het RIVM zijn gedocumenteerd ('opzet');
- Deze maatregelen daadwerkelijk zijn getroffen ('bestaan');
- Deze maatregelen voldoen aan de BIO;
- Deze maatregelen BBN2 realiseren of al BBN3 mogelijk maken.

Wij hebben geen onderzoek gedaan naar de operationele effectiviteit ('werking') van de beheersingsmaatregelen.

De bevindingen vanuit onze werkzaamheden en de daaruit voortvloeiende adviezen zijn opgenomen in het bovenstaande hoofdstuk 'Management samenvatting'.

2.4. *Overzicht van de adviezen*

De in dit rapport opgenomen adviezen zijn hieronder samengevat. Wij maken in de kolom 'Prioriteit' onderscheid tussen al lopend, korte termijn (binnen 6 maanden), middellange termijn (tussen 6 en 12 maanden) en lange termijn.

Sectie	Advies	Prioriteit
1.3	**Aanvullende off-line back-up** Wij adviseren naast on-line back-up tevens een periodieke off-line back-up in te richten met verschillende retentieperiodes, gezien de recente ransomware-aanvallen op de overheid. Bij een juiste inrichting van de aanvullende off-line back-up is CIMS op een robuustere wijze bestand tegen ransomware.	Korte termijn
1.4	**Eigenaarschap** Wij adviseren de inrichting van het eigenaarschap van de CIMS-omgeving te documenteren in relatie tot het VIR-BI, zodat aantoonbaar wordt dat het eigenaarschap op niveau BBN3 ligt.	Middellange termijn
1.4	**Logische toegangsbeveiliging van de CIMS-omgeving** Wij adviseren prioriteit te geven aan het inventariseren en inrichten van het accountbeheer voor de CIMS-omgeving, bij voorkeur op niveau BBN3. Het accountbeheerproces dient geheel te worden beschreven en te voldoen aan de VIR-BI-eis 'minste privilege'. Tevens dient monitoring via SIEM/SOC te worden ingericht.	Korte termijn
1.4	**De levenscyclus van de CIMS-omgeving** Wij adviseren de inrichting van risicobeheersing en de planning van audits voor de CIMS-omgeving te documenteren in relatie tot het VIR-BI, zodat aantoonbaar wordt dat de levenscyclus op niveau BBN3 ligt.	Middellange termijn
1.5	**Gebruik van bestanden met Comma Separated Value (csv)** Wij adviseren technische maatregelen te treffen om de vertrouwelijkheid en integriteit van csv-bestanden te borgen binnen de keten, in samenwerking met de ketenpartners.	Korte termijn
1.6	**Systemen binnen de keten voor CIMS** Wij adviseren quick scans uit te laten voeren op compliance met de BIO voor de belangrijkste systemen binnen de keten, te starten met CoronIT en de ODBC-koppeling met CIMS.	Korte termijn
3.3	**Logische toegangsbeveiliging** Wij adviseren, in het kader van de op dit moment nog beperkte monitoring op de logische toegangsbeveiliging, om maandelijks analyses te laten uitvoeren op de autorisatiematrix in de RIVM Active Directory (AD) en de autorisatiematrix van CIMS. Hierbij dient te worden gecontroleerd dat er alleen accounts zijn op basis van 'need to have' en met de laagst mogelijke privileges.	Korte termijn

2.5. *Vrij gebruik van het rapport en de verspreidingskring*

Bij het opstellen van deze rapportage is rekening gehouden met de verwachtingen van de beoogde gebruikers, namelijk de burgers en de volksvertegenwoordiging, en de eis van de opdrachtgever dat publieke verificatie mogelijk moet zijn. Daarom is deze rapportage zo opgezet dat deze publiekelijk kan worden gedeeld.

Hazerswoude, 8 januari 2021

5.1.2e

5.1.2e

3. Detailrapport: Waarnemingen en conclusies per aandachtsgebied

Wij hebben de in bijlage A genoemde functionarissen geïnterviewd of gesproken, en de in bijlage B genoemde documenten bestudeerd.

Wij hebben waarnemingen voor de fysieke beveiliging uitgevoerd op een locatie van Equinix. Onze waarnemingen en conclusies zijn hieronder per aandachtsgebied uitgewerkt.

Het door ons ontwikkelde werkprogramma voor het inventariseren van de beheersingsmaatregelen in relatie tot de eisen voor informatiebeveiliging is gericht op het verkrijgen van de mate van inzicht dat nodig is voor het leveren van publieke transparantie. De aanpak en het werkprogramma zijn voorafgaand aan het onderzoek afgestemd met de opdrachtgever. De bevindingen zijn in concept afgestemd met de opdrachtgever.

In de onderstaande tekst refereren wij aan de documentatie in de vorm van '[doc x]', waarbij 'x' ons dossiernummer is van een door ons ontvangen en bestudeerd document.

3.1. Informatie binnen CIMS

Wij hebben de volgende documentatie gereviewed:

1	Gezamenlijke notitie RIVM, Lareb en VWS, Centraal register COVID vaccinatie	22-12-2020
2	Pels Rijcken, Landsadvocaat, Voorlopige definitieve DPIA CIMS	18-12-2020
3	FG VWS, (Tussen)Advies DPIA CIMS	17-12-2020
4	VWS, Spoedadvies informatiebeveiliging CIMS Beveiligingsaspecten	14-12-2020

In de gezamenlijke notitie van RIVM, Lareb en VWS, 'Centraal register COVID vaccinatie' [doc 1] is het proces van informatieverstrekking beschreven, evenals een specificatie van de gegevens.

In sommige (gedateerde?) documenten wordt gesteld dat vanuit CIMS uitnodigingen zullen worden opgesteld voor vaccinatie. Dit is echter niet het geval voor CIMS release 1, welke alleen wordt gebruikt voor registratie en monitoring. Uitnodigingen worden opgesteld door andere instanties, zoals Arbo-diensten en huisartsen, en worden niet gedeeld met het RIVM. In de toekomst kan dit veranderen bij een hoger release van CIMS, bijvoorbeeld op het moment dat restgroepen moeten worden uitgenodigd.

Een Data Protection Impact Analyse (DPIA) [doc 2] is beschikbaar, evenals een eerste reactie daarop van de Functionaris voor de Gegevensbescherming van het ministerie van VWS [doc 3].

Er is een intern spoedadvies [doc 4], waarin onder andere de risico's zijn aangegeven van het gebruik van csv-bestanden, gebrek aan monitoring etc. Deze risico's zijn meegenomen in de risicoanalyses van het RIVM.

Ten tijde van ons onderzoek waren de gegevens vanuit de Basisregistratie Personen (BRP) geladen, conform een autorisatiebesluit van de Rijksdienst voor Identiteitsgegevens (RvIG). Via een

abonnement op bepaalde gegevensvelden in de BRP wordt de informatie in CIMS actueel gehouden. Informatie vanuit de Registratie Niet Ingezetenen (RNI) en het Centraal Orgaan Opvang Asielzoekers (COA) worden op een soortgelijke wijze verwerkt.

Gegevens vanuit de geautomatiseerde basisadministratie met persoonsgegevens over geprivilegieerden (Probas) zijn nog niet opgenomen in CIMS.

Onze vraag over het gebruik van geanonimiseerde testgegevens in de Ontwikkel – Test – Acceptatie – Productie omgevingen, de zogenaamde OTAP-straat, kon tijdens de interviews niet worden beantwoord.

3.2. Risicobeheersing voor CIMS

Wij hebben de volgende documentatie gereviewed:

6	RIVM spreadsheet, CIMS Issue actielijst P IB, versie 1.2	17-12-2020
7	RIVM spreadsheet, Risicoanalyse CIMS, versie 1.2	17-12-2020
8	Stuurgroep Registratie COVID vaccinatie programma, Risicoregister CIMS, versie 1.0	20-12-2020
9	RIVM, Risicomatrix CIMS	05-12-2020
10	NCSC, Opmerkingen risicoanalyse CIMS	17-12-2020
11	RIVM, Handboek Informatiebeveiliging, versie 0.96a1	05-10-2020

De spreadsheet 'CIMS Issue actielijst' [doc 6] is een vastlegging van de te nemen maatregelen, de (rest)risico's, referenties naar de relevante BIO-normen, belegging van de verantwoordelijkheden en een vastlegging van de voortgang. Een aantal van de genoemde acties staat genoteerd met een opleveringsdatum van 30 december 2020. Dit valt na ons onderzoek, waardoor wij niet in staat zijn om de realisatie te verifiëren.

De spreadsheet 'Risicoanalyse CIMS' is opgezet conform de standaard NEN-ISO/IEC 27005 'Guidelines for information security risk management' [doc 7]. Het bevat 11 tabbladen met onder andere een analyse van de dreigende actoren, kwetsbaarheden, kansen, impact en risico's. Dit resulteert in een overzicht van de risico's in het document 'Risicomatrix CIMS' [doc 9].

Het Nationaal Cyber Security Centrum (NCSC) heeft een document 'Opmerkingen risicoanalyse CIMS' [doc 10] opgesteld, met een aantal nuttige adviezen. Hierin wordt onder andere gesteld dat het RIVM ervoor dient te zorgen dat ransomware niet de back-up kan raken. Dit punt hebben wij meegenomen bij onze adviezen.

In het 'Handboek Informatiebeveiliging' [doc 11] wordt de volgende aanpak voorgeschreven: '*Binnen risicobeheer kan de identificatie van veiligheidsrisico's en de selectie van beveiligingsmaatregelen worden uitgevoerd met behulp van verschillende risicobeheer normen, zoals onder andere ISO 31000:2018, Risicobeheer – Richtlijnen en ISO27005:2011, Information security risk management. In grote lijnen bestaat het door dit Handboek gebruikte risicobeheerraamwerk uit zes stappen: definieer het systeem, selecteer beveiligingsmaatregelen, implementeer beveiligingsmaatregelen, beoordeel beveiligingsmaatregelen, autoriseer het systeem en bewaak het systeem*'.

Wij hebben bij onze desk research en interviews geen afwijkingen geconstateerd voor de aanpak van risicobeheersing voor de CIMS-omgeving, die is uitgevoerd conform de richtlijnen in het 'Handboek Informatiebeveiliging' [doc 11].

3.3. Logische toegangsbeveiliging

Wij hebben de volgende documentatie gereviewed:

6	RIVM spreadsheet, CIMS Issue actielijst P IB, versie 1.2	17-12-2020
23	Ordina, Verwerkersovereenkomst RIVM DVP	11-10-2018
25	RIVM, DVP SOP 0711 Procedure aanvraag account	-
26	RIVM, Aanvraag-wijzigingsformulier Praeventis BRP CIMS gebruikersaccount	-
46	RIVM spreadsheet, CIMS Rollen en rechten per tabel, versie 0.1	23-12-2020

De rollen en bevoegdheden binnen CIMS zijn deels gekopieerd vanuit het Praeventis-systeem. Er lopen nog acties voor het inventariseren en inrichten van het accountbeheer. Deze acties zijn deels beschreven in de spreadsheet 'CIMS Issue actielijst' [doc 6], evenals de datum waarop deze moeten worden gerealiseerd.

Met de IT-dienstverlener Ordina is een 'Verwerkersovereenkomst RIVM DVP' [doc 23] afgesloten, waarin de AVG-vereisten zijn behandeld.

De 'Procedure aanvraag account' [doc 25] is incompleet en verouderd. Deze had uiterlijk op 29-11-2018 moeten worden herzien.

Tijdens de interviews hebben wij vernomen dat de VIR-BI-eis 'minste privilege' niet is meegenomen in de plannen voor het structureren van het accountbeheerproces voor CIMS. Onze vraag of de VIR-BI-eis voor 'maximaal 5 mislukte inlogpogingen bij CIMS' is gerealiseerd, kon niet worden beantwoord.

In de spreadsheet 'CIMS Issue actielijst' [doc 6] staat dat monitoring via SIEM/SOC nog moet worden ingericht.

Er wordt geen gebruik gemaakt van Single Sign-On (SSO). Een RIVM-medewerker moet eerst inloggen op het RIVM-netwerk via de Active Directory, en vervolgens separaat inloggen op CIMS. Als een medewerker van buiten kantoor werkt, moet gebruik worden gemaakt van Two Factor Authentication (TFA).

Een belangrijke compenserende beveiligingsmaatregel is het feit dat CIMS release 1 alleen toegankelijk is voor geautoriseerde medewerkers van het RIVM, en niet voor derde partijen. Indien een andere instantie gegevens nodig heeft, moeten die worden aangevraagd bij het RIVM.

Wij adviseren, in het kader van de op dit moment nog beperkte monitoring op de logische toegangsbeveiliging, om maandelijks analyses te laten uitvoeren op de autorisatiematrix in de RIVM Active Directory (AD) en de autorisatiematrix van CIMS. Hierbij dient te worden gecontroleerd dat er alleen accounts zijn op basis van 'need to have' en met de laagst mogelijke privileges.

3.4. *Fysieke toegangsbeveiliging*

Wij hebben het datacenter van Equinix met de CIMS-omgeving bezocht. Conform onze afspraak met het RIVM hebben wij geen foto's of video's gemaakt, alleen aantekeningen.

In het datacenter staat een kooi met de racks, waarvoor strikte toegangsregels gelden. Er wordt gebruik gemaakt van het vier-ogen-principe, waardoor nooit één partij alleen toegang heeft.

Wij hebben geen afwijkingen geconstateerd voor de fysieke beveiligingsmaatregelen, conform het VIR-BI. Aangezien dit gedeelte van het datacenter regelmatig wordt geaudit namens de bevoegde instanties, kunnen de fysieke beveiligingsmaatregelen voor de CIMS-omgeving worden gezien als BBN3.

3.5. *Communicatiebeveiliging*

Wij hebben de volgende documentatie gereviewed:

24	RIVM presentatie, De wereld van CIMS volgens de architecten, versie 1	15-12-2020
28	RIVM presentatie, RIVM koppelingen, versie 1.5	15-07-2020
31	RIVM, Praeventis TO Hosting AHP_032, versie 0.9.3	31-05-2020
32	RIVM spreadsheet, Preaventis Integration characteristics, versie 1.3	29-07-2020
33	RIVM, Praeventis Integration DPV_058, versie 1.3.0.1	13-08-2020
34	RIVM Visio, Praeventis Externe verbindingen	06-12-2019
41	RIVM, CIMS TO Hosting, versie 0.91	09-12-2020
42	RIVM presentatie, CIMS Systeemdecomposities, versie 2	19-12-2020
43	RIVM presentatie, CIMS Aansluitscenario's DPV_188	16-12-2020
44	RIVM, CIMS Koppelingen DPV_161, versie 1.1	07-12-2020
45	RIVM, CIMS Koppeling GGD GHOR DPV_189	18-12-2020

Ten tijde van ons onderzoek was CIMS release 1 nog in opbouw, en bleek de documentatie van de externe verbindingen achter te lopen op de realiteit. Gezien de hoge tijdsdruk met de krappe deadline voor de inproductiename is dat begrijpelijk.

Hierdoor hebben wij echter geen compleet beeld kunnen vormen van de risico's voor datacommunicatie. Niettemin hebben wij tijdens de interviews wel aandacht kunnen besteden aan de uitwisseling van de csv-bestanden en de koppeling met CoronIT van GGD GHOR.

De meeste communicatieverbindingen met de CIMS-omgeving zijn volgens de geïnterviewden voorzien van veilige protocollen en mechanieken.

3.5.1. *Uitwisseling van gegevens via csv-bestanden*

Een uitzondering hierop vormt de server voor het Secure File Transfer Protocol (SFTP) en de mailbox voor E-Zorg. De SFTP-server en mailbox worden gebruikt voor het transport van bestanden met het formaat Comma Separated Value (csv) van en naar ketenpartners. In principe is

het mogelijk dat deze bestanden ergens in de keten op een ongeautoriseerde wijze worden gekopieerd of worden gemanipuleerd.

Het RIVM is bezig een Gateway in te richten voor Application Programming Interface (API), waarbij de informatieuitwisseling op een veilige manier kan plaatsvinden. Deze aanpak is beschreven in 'CIMS Aansluitscenario's DPV_188' [doc 43].

Niettemin vereist het gebruik van de API Gateway technische aanpassingen bij ketenpartners. Het blijkt dat niet alle ketenpartners in staat zijn gebuik te maken van deze veilige wijze van informatieuitwisseling.

Wij adviseren technische maatregelen te treffen om de vertrouwelijkheid en integriteit van csv-bestanden te borgen binnen de keten, in samenwerking met de ketenpartners.

3.5.2. Uitwisseling van vaccinatiegegevens met GGD GHOR

Voor CIMS release 1 hebben wij vernomen dat het systeem CoronIT van GGD GHOR wordt aangesloten via een ODBC-koppeling op een Postgress-afslag van de database van CoronIT, via een Virtual Private Network (VPN). Dit is beschreven in 'CIMS Koppeling GGD GHOR DPV_189' [doc 45].

CoronIT wordt gebruikt door de 25 GGD-regio's bij het vaccinatieprogramma.

Wij hebben echter geen assurance dat voor systemen binnen de keten eenzelfde niveau van informatiebeveiliging is geborgd als voor de CIMS-omgeving.

Wij adviseren quick scans uit te laten voeren op compliance met de BIO voor de belangrijkste systemen binnen de keten, te starten met CoronIT en de ODBC-koppeling met CIMS.

Bijlage A Overzicht van gesprekken en waarneming

In het kader van de privacy van de geïnterviewde en betrokken functionarissen zijn hieronder alleen hun functies benoemd.

Nr.	Functie	Datum
1.	Directeur Informatiebeleid en CIO, Ministerie van VWS	22-12-2020
2.	Chief Security & Privacy Operations (CSPO), Programma Realisatie Digitale Ondersteuning, Ministerie van VWS	22-12-2020
3.	Directeur IV / CIO, RIVM	24-12-2020
4.	Chief Information Security Officer (CISO) (a.i.), RIVM	22-12-2020 23-12-2020
5.	Information Security Officer (ISO), RIVM	E-mails
6.	Coördinator, Ontwikkelteam CIMS, RIVM	23-12-2020
7.	Programma Manager, Ontwikkelteam CIMS, RIVM	23-12-2020 24-12-2020
8.	Afdelingshoofd ICT Basisdiensten (a.i.), SSC Campus, RIVM	23-12-2020
9.	Afdelingshoofd Basisinfrastructuur (a.i.), SSC Campus, RIVM	24-12-2020

Nr.	Waarneming	Datum
1.	Locatiebezoek bij het Equinix Datacenter	24-12-2020

Bijlage B Lijst van geraadpleegde documentatie

Wij hebben de volgende documentatie ontvangen:

Nr.	Dossierstuk	Datum
1	Gezamenlijke notitie RIVM, Lareb en VWS, Centraal register COVID vaccinatie	22-12-2020
2	Pels Rijcken, Landsadvocaat, Voorlopige definitieve DPIA CIMS	18-12-2020
3	FG VWS, (Tussen)Advies DPIA CIMS	17-12-2020
4	VWS, Spoedadvies informatiebeveiliging CIMS Beveiligingsaspecten	14-12-2020
5	RIVM, DPV Overzicht procesdocumentatie CIMS privacy	21-12-2020
6	RIVM spreadsheet, CIMS Issue actielijst P IB, versie 1.2	17-12-2020
7	RIVM spreadsheet, Risicoanalyse CIMS, versie 1.2	17-12-2020
8	Stuurgroep Registratie COVID vaccinatie programma, Risicoregister CIMS, versie 1.0	20-12-2020
9	RIVM, Risicomatrix CIMS	05-12-2020
10	NCSC, Opmerkingen risicoanalyse CIMS	17-12-2020
11	RIVM, Handboek Informatiebeveiliging, versie 0.96a1	05-10-2020
21	Kamerbrief, BIT advies programma Vernieuwd Praeventis	19-02-2019
22	BIT, Advies programma Vernieuwd Praeventis	17-01-2019
23	Ordina, Verwerkersovereenkomst RIVM DVP	11-10-2018
24	RIVM presentatie, De wereld van CIMS volgens de architecten, versie 1	15-12-2020
25	RIVM, DVP SOP 0711 Procedure aanvraag account	-
26	RIVM, Aanvraag-wijzigingsformulier Praeventis BRP CIMS gebruikers-account	-
27	RIVM, Use Case covidvaccinatie, versie 0.8	01-12-2020
28	RIVM presentatie, RIVM koppelingen, versie 1.5	15-07-2020
31	RIVM, Praeventis TO Hosting AHP_032, versie 0.9.3	31-05-2020
32	RIVM spreadsheet, Preaventis Integration characteristics, versie 1.3	29-07-2020
33	RIVM, Praeventis Integration DPV_058, versie 1.3.0.1	13-08-2020
34	RIVM Visio, Praeventis Externe verbindingen	06-12-2019
41	RIVM, CIMS TO Hosting, versie 0.91	09-12-2020
42	RIVM presentatie, CIMS Systeemdecomposities, versie 2	19-12-2020
43	RIVM presentatie, CIMS Aansluitscenario's DPV_188	16-12-2020
44	RIVM, CIMS Koppelingen DPV_161, versie 1.1	07-12-2020
45	RIVM, CIMS Koppeling GGD GHOR DPV_189	18-12-2020
46	RIVM spreadsheet, CIMS Rollen en rechten per tabel, versie 0.1	23-12-2020
47	RIVM presentatie, CIMS Backup en DB encryptie voorstel	18-12-2020
51	RIVM presentatie, Kamerbriefing Van Dissel directeur Centrum Infectie-ziektebestrijding RIVM	18-11-2020
52	Gezondheidsraad, Advies Strategieën voor COVID-19 vaccinatie	19-11-2020
53	Kamerbrief, COVID-19 vaccinatiestrategie	20-11-2020
54	CBG over Kamerbrief COVID-19 vaccinatiestrategie	20-11-2020
55	Kamerbrief, Uitwerking vaccinatiestrategie COVID-19	21-12-2020

Bijlage C Lijst van afkortingen

Afkorting	Toelichting
AD	Active Directory, Microsoft
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
BBN	Basisbeveiligingsniveau conform de BIO
BIO	Baseline Informatiebeveiliging Overheid
CIMS	COVID-vaccinatie Informatie- en Monitoringsysteem
CISO	Chief Information Security Officer
CMDB	Configuration Management Data Base
CSPO	Chief Security & Privacy Operations
DPIA	Data Protection Impact Analyse (identiek aan GEB)
DV	Departementaal Vertrouwelijk
FG	Functionaris voor de Gegevensbescherming
GGD GHOR	Gemeentelijke Gezondheidsdienst en Geneeskundige Hulpverleningsorganisatie in de Regio
ICT	Informatie en Communicatie Technologie
IDU	Instroom, Doorstroom en Uitstroom
ISAE	International Standard on Assurance Engagements
ITGC	IT General Controls
ODBC	Open DataBase Connectivity
OTAP	Ontwikkel, Test, Acceptatie en Productie
RIVM	Rijksinstituut voor Volksgezondheid en Milieu
SIEM	Security Information & Event Monitoring
SOC	Security Operating Center
SSO	Single Sign-On
TFA	Two Factor Authentication
VIR-BI	Voorschrift Informatiebeveiliging Rijksoverheid – Bijzondere Informatie
VPN	Virtual Private Network. Dit is een versleutelde verbinding over internet.
VWS	Ministerie van Volksgezondheid, Welzijn en Sport

Documentbeheer

Doelgroep: Directie RIVM en ministerie van VWS

Versie	Datum	Naam	Verandering
0.01	22-12-2020	5.1.2e	Initiële opzet
0.02	23-12-2020		Desk research
0.03	25-12-2020		Verwerken interviews en waarneming
0.80	26-12-2020	5.1.2e	Kwaliteitscontrole
0.90	27-12-2020	5.1.2e	Semi definitieve versie
1.00	08-01-2021	5.1.2e	Finaliseren

Review en accordering

Versie	Datum	Reviewer	Status en doel
0.80	27-12-2020	5.1.2e	OK
0.80	27-12-2020	5.1.2e	OK
0.90	08-01-2021	5.1.2e	OK