Quickscan BIO XXXX

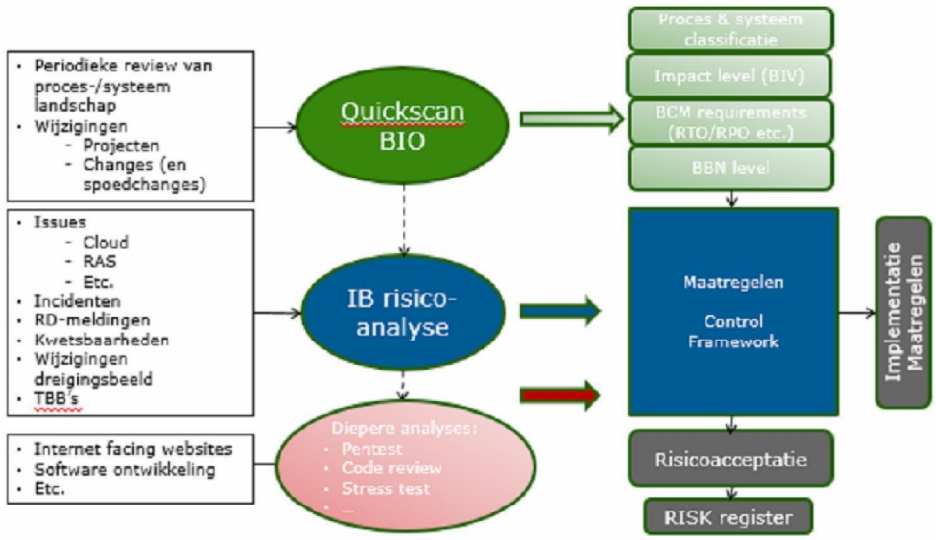
<CliëntPortaal RIVM – CIMS (Final draft)>

De Quickscan Information Security (QIS), kortweg Quickscan BIO, is het hulpmiddel om het basisbeveiligingsniveau (BBN) vast te stellen. Het is de BBN-toets zoals beschreven in de BIO. Daarnaast worden met de quickscan de proces- en systeemclassificatie en het impactniveau op basis van de betrouwbaarheidseisen vastgesteld evenals de Business Continuity Management (BCM) eisen. Dit laatste op basis van de:

- Recovery Point Objective (RPO); maximaal toelaatbare hoeveelheid dataverlies;
- Recovery Time Objective (RTO); maximale benodigde hersteltijd.

Daarnaast worden eventuele aanvullende vereisten bepaald die noodzakelijk zijn om een informatiesysteem te beschermen gegeven het belang dat de eigenaar daaraan toekent. Behoudens de BBN-toets kunnen alle stappen in de quickscan waar gewenst worden aangevuld en aangepast om de aansluiting van de quickscan op de praktijk van de eigen organisatie te bevorderen.

De quickscan wordt periodiek uitgevoerd en bij grote wijzigingen op het proces en/of informatiesysteem in projecten. Het resultaat van de Quickscan wordt vastgesteld door de eigenaar van het proces en/of informatiesysteem. Zie bijlage A voor een toelichting per stap.



STAP 1: Bepaal scope, context en rubricering

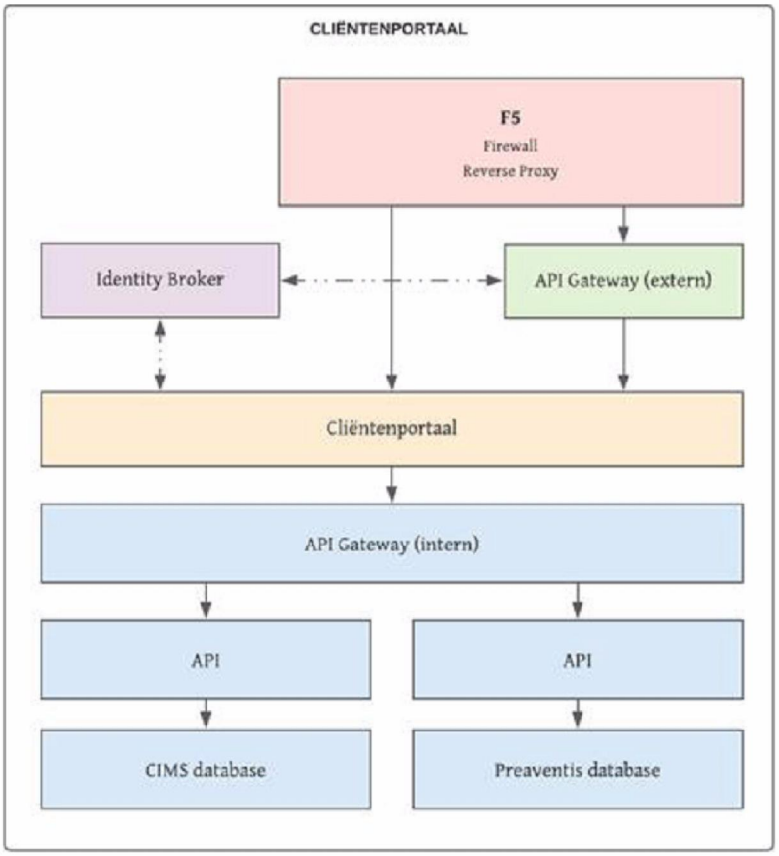
		<Proces A> Cliëntportaal
		Korte beschrijving van het proces Externe gebruikers (burgers) elektronische toegang verlenen tot RIVM diensten. "Digitale toegangspoort naar het RIVM voor burgers". (PSA, par 2.2, 2.3 P6).
A	<Informatiesysteem 1> **Cliëntportaal – met koppeling naar CIMS**	*Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces* Het aan de burger digitaal toegang geven tot RIVM diensten. De eerste koppeling is CIMS: COVID-19 vaccinatie Informatie- en Monitoringsysteem.
	<Informatiesysteem 2> **RIVMToegang**	*Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces* RIVMToegang is het systeem dat de authenticatie en authorisatie onzichtbaar voor de klant afhandelt. **Buiten scope, zie eigen QuickScan en RisicoAnalyse.**
	<Informatiesysteem 3> **CIMS: COVID-19 vaccinatie Informatie- en Monitoringsysteem**	*Beschrijving van de ondersteunende functie van het informatiesysteem voor het procesonzichtbaar voor de Client afhandeld.* De eerste dienst die aangesloten wordt op Cliëntportaal is de CIMS vaccinatiegegevens en planning van de burger (CIMS: COVID-19 vaccinatie Informatie- en Monitoringsysteem) en zal via Clientportaal electronisch toegankelijk zijn. **Buiten scope, zie eigen QuickScan en RisicoAnalyse.**
	<Informatiesysteem 4> **DigID**	*Beschrijving van de ondersteunende functie van het informatiesysteem* De burger wordt gevraagd in te loggen met DigID voor identificatie en authenticatie. **Buiten scope, zie eigen QuickScan en RisicoAnalyse.**
	<Informatiesysteem 4> **Interne API manager**	*Beschrijving van de ondersteunende functie van het informatiesysteem* De Interne API manager regelt de toegang tot achterliggende RIVM diensten, onzichtbaar voor de klant. **Buiten scope, zie eigen QuickScan en RisicoAnalyse.**

B	*<Naam van proces A> Cliëntportaal*	
	De klant van het proces	*De klant is degene die direct aan het eind van het proces het resultaat (de output) afneemt:* - *<wie is de interne klant?>* **RIVM centra en hun diensten die toegankelijk voor de burger zijn met als eerste dienst CIMS: COVID-19 vaccinatie Informatie- en Monitoringsysteem.** - *<wie is de externe klant?>* **Burgers ingeschreven in Nederland.**
	De output van het proces	*<De output is het resultaat van handelen in het proces>* **Geauthentiseerde en geautoriseerde elektronische / digitale toegang tot RIVM diensten verlenen.**
	Koppelvlakken met andere processen	- *<aanleverende processen/organisaties>* **RIVM Vaccinatiegegevens en planning CIMS.** - *<afnemende processen/organisaties>* **Informatie geleverd aan de burgers.**
	Gebruikte systemen	- *De informatiesystemen die worden gebruikt bij de activiteiten in het proces:* - *<informatiesysteem>* **RIVMToegang, API interne Manager, CIMS.**

<Ingeval van meerdere processen kopieer blok B>

C	*<Naam van het Informatiesysteem 1> Cliëntportaal*	
	Eigenaar informatiesysteem	*<naam van de eigenaar van het informatiesysteem>* **DVP,** 5.1.2e 5.1.2e 5.1.2e
	De gebruikers van het informatiesysteem	- *Degene die werkzaam zijn met het informatiesysteem* - *<wie is de interne gebruiker / klant?>* **RIVM diensten** - *<wie is de externe gebruiker / klant?>* **Burgers** - *<aantal gebruikers / burgers>* **Gehele bevolking >16 jaar**
	De output van het informatiesysteem	**Informatie uit RIVM systeem CIMS (COVID-19 vaccinatie Informatie- en Monitoringsysteem).** **Dit is de eerste dienst die op Cliëntportaal aangesloten wordt.**
	Koppelvlakken met andere informatiesystemen	*Een architectuurplaatje kan hier verhelderend werken.* **Zie architectuurplaat.**
	Andere processen	*Welke andere processen worden door het informatiesysteem ondersteund?* **Geen.**
	Kritische momenten	*Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes.* **24x7 exclusief onderhoud (patch/servicewindow op donderdagavond en ongeplande verstoring). Verstoringen na 20 uur 'savonds worden pas de volgende dag opgepakt.**
	Soort informatie	- *Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?)* - **Privacygevoelige informatie (persoonsgegevens en bijzondere persoonsgegevens medische gegevens).**
	Data rubricering[1]	*Welke classificatie is van toepassing op de informatie? (Openbaar, XXXX intern, XXXX vertrouwelijk, Departementaal Vertrouwelijk, Stg. Confidentieel, Stg. Geheim, Stg Zeer Geheim)* **RIVM Vertrouwelijk.**
	Externe eisen	*Denk hierbij aan eisen vanuit de AVG, NAVO, EU, ketenpartner(s) en evt. andere organisatie(s).* **AVG, EU. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg – WABVPZ.**

Architectuurplaat


CLIËNTENPORTAAL
F5
Firewall
Reverse Proxy
Identity Broker
API Gateway (extern)
Cliëntenportaal
API Gateway (intern)
API
API
CIMS database
Preaventis database

STAP 2: Classificeer proces en informatiesysteem en bepaal externe eisen

D	Classificatie van de processen	
	Ondersteunend (O)	**Voorwaardenscheppend**
	De activiteiten waaraan de typering 'handig om te hebben' kan worden toegekend Deze activiteiten hebben geen directe relatie naar het voortbrengen van de producten/diensten waaraan de instelling haar bestaansrecht ontleent. In de meeste gevallen is hier sprake van een ondersteunende rol naar de lijn. De activiteiten vormen een waardevolle support van het primaire proces.	
	Bijdragend (B)	**Subtaak**
	Er is slechts sprake van een indirecte relatie met de hoofdactiviteiten van het ministerie/kerndepartement of uitvoeringsorganisatie. Het ontbreken echter van het 'bijdragende proces' heeft echter wel effectiviteits- en efficiencyverliezen binnen het primaire proces effectiviteit- en efficiencyverliezen tot gevolg.	
	Strategisch (S)	**Afgeleide kerntaak**
	• Het proces heeft een directe relatie met het uitvoeren van de doelstellingen van het ministerie/ kerndepartement of uitvoeringsorganisatie. Het betreft het primaire proces van de directie, agentschap, raad, etc. • Aan het proces kan een ontwikkelpotentieel worden toegekend. Met andere woorden, het wordt in de toekomst belangrijker in verband met mogelijke veranderingen in de strategische doelstellingen van het ministerie/kerndepartement ofuitvoeringsorganisatie. • Een aanzienlijk deel van de omzet (50% - 80%) wordt gegenereerd met dit proces of een aanzienlijk deel (50% - 80%) van het te besteden budget komt ten goede aan ditproces. Het proces heeft te maken met de uitvoering van wettelijke taken (het betreft hier primaire processen met wettelijk/ contractueel vastgelegde termijnen).	
	Kritisch strategisch (K)	**Kerntaak**
	• In relatie tot de doelstellingen van het ministerie/ kerndepartement of uitvoeringsorganisatie speelt het bedrijfsproces een primaire rol. Het hoort bij de primaire taken waarop het ministerie/kerndepartement of uitvoeringsorganisatie direct kan worden aangesproken. Het ministerie/kerndepartement of uitvoeringsorganisatie ontleent haar bestaansrecht aan het uitvoeren van deze taken. Het betreft een maatschappelijk vitaal proces. Deze vitale belangen zijn territoriale-, fysieke-, economische-, en ecologische veiligheid en sociale en politieke stabiliteit. • De instelling krijgt 80% of meer van de inkomsten uit dit proces, c.q. het budget van de organisatie wordt voor meer dan 80% uitgeput door dit proces. • Als de activiteit langer dan één week stilvalt of niet goed verloopt, heeft dit ernstige gevolgen voor het voortbestaan van de organisatie, c.q. het brengt het ministerie/kerndepartement of uitvoeringsorganisatie in een hachelijke positie.	

Procesnaam	Classificatie proces O, B, S, K	Toelichting
<Proces A> Cliëntportaal	*B*	*Dit is geen strategisch doel, bij nieuwe koppelingen opnieuw QuickScan uitvoeren. Bijdragend omdat diensten ook nog op een andere manier benaderbaar blijven.*

E	Classificatie van de informatiesystemen	
	Typering	**Waardering**
	• **Nuttig (N)** •	Het informatiesysteem geeft support bij de activiteiten binnenhet bedrijfsproces en is 'handig om te hebben'.
	Belangrijk (B)	- Het informatiesysteem levert een belangrijke bijdrage aan de activiteiten binnen het proces en/of de levering van de producten ofdiensten. - Slechts met grote, onevenredige inspanning is voortzetting van het proces mogelijk. - Inzet van het informatiesysteem heeft een positief effect op de doeltreffendheid en doelmatigheid van de organisatie. - Het informatiesysteem wordt door veel (interne/externe) medewerkers/burgers gebruikt.
	- **Vitaal (V)**	- Het uitvoeren van de bedrijfsprocessen of het tot stand brengen van producten/diensten is (nagenoeg) onmogelijk zonder de inzet van het informatiesysteem. - Inzet van het informatiesysteem is essentieel voor een goede uitvoering van het bedrijfsproces.

Informatiesysteemnaam	*Classificatie systeem N, B, V*	*Toelichting*
Cliëntportaal	*N*	*Nu Nuttig omdat andere communicatie als per brief nog mogelijk blijft.*
RIVMToegang (Bron: Quickscan BIO RIVMToegang - v1.0)	*V*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
CIMS: COVID-19 vaccinatie Informatie- en Monitoringsysteem	*V*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*

DigID	V	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
Interne API Manager	V	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*

STAP 3: Bepaal betrouwbaarheidseisen

F	Impactclassificatie voor beschikbaarheid			
	Impact	**Imagoschade** *Publieke reputatie, vertrouwen*	**Financiële schade** *Additionele kosten*	**Uitval schade** *Operatie*
	Laag *RTO max. **5** dagen* *RPO max. **28** uur* *Beschikbaar **99%***	• Irritaties en ongemak burgers geventileerd in media • Interne negatieve publiciteit	• Op te vangen binnen de begroting van ministerie of XXXX	• Max 2 weken (incl. piek) • Beperkt verlies van management control
	Midden *RTO max. **2** dagen* *RPO max. **24** uur* *Beschikbaar **99,5%***	• Verlies van publiek respect • Klachten van burgers • Rijksbrede negatieve publiciteit • Verlies aan motivatie medewerkers	• Niet op te vangen binnen de begroting van ministerie of XXXX • Accountantsverklaring niet afgegeven	• Max 1 week (incl. piek) • Belangrijk verlies van management control
	Hoog *RTO =**<2** dagen* *RPO =**<24** uur* *Beschikbaar **>=99,9%***	• Ernstigere schade dan het bij "Midden" beschreven schadescenario • De beschikbaarheidseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren • In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken		

Informatiesysteem	**Classificatie informatie** *Laag, Midden, Hoog*	**RPO & RTO**	**Toelichting**
Cliëntportaal	*H*	*RTO =**<2** dagen* *RPO =**<24** uur* *Beschikbaar >98.5%*	*RTO: 98,5%, dit is de RIVM standaard vanwege de service/patch window 1x per maand op donderdag en de afspraak van geen ondersteuning in de nacht na 20.00 s'avonds in het geval van een issue.* *RTO: context vooral politiek gevoelig ivm reputatie. Beheerplan met IV organisatie.* *RPO (Recovery Point Objevtive) niet van toepassing, want er wordt geen data opgeslagen die verloren kan gaan.*
RIVMToegang *(Bron: Quickscan BIO RIVMToegang - v1.0)*	*H*	*RTO: < 2 dagen* *RPO: Nvt, geen opslag van data.* *99,9% beschikbaar*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
CIMS: COVID-19 vaccinatie Informatie- en Monitoringsysteem	*H*	*RTO: < 2 dagen* *RPO: <24 uur* *99,9% beschikbaar*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
DigID	*H*	*RTO: < 2 dagen* *RPO: <24 uur* *99,9% beschikbaar*	*Buiten scope voor deze QuickScan.*
Interne API Manager	*H*	*RTO: < 2 dagen* *RPO: <24 uur* *99,9% beschikbaar*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*

G	Impactclassificatie voor integriteit			
	Impact	**Imagoschade** *Publieke reputatie, vertrouwen*	**Financiële schade** *Additionele kosten*	**Uitval schade** *Operatie*
	Laag *Beperkte schade*	• Irritaties en ongemak burgers geventileerd in media • Interne negatieve publiciteit	• Op te vangen binnen de begroting van ministerie of XXXX	• Beperkt verlies van management control
	Midden *Forse schade*	• Verlies van publiek respect • Klachten van burgers • Rijksbrede negatieve publiciteit • Verlies aan motivatie medewerkers	• Niet op te vangen binnen de begroting van ministerie of XXXX • Accountantsverklaring niet afgegeven	• Belangrijk verlies van management control
	Hoog	• Ernstigere schade dan het bij "Midden" beschreven schadescenario • De integriteitseis overstijgt het standaard niveau dat een dienstenleverancier op dit moment kan leveren • In overleg met een dienstenleverancier moeten specifiek voor de situatie benodigde maatregelen worden afgesproken		

Informatie/systeem	Classificatie informatie *Laag, Midden, Hoog*	Toelichting
Cliëntportaal	*M*	*Voor ClientPortaal kijken wij naar de te koppelen dienst CIMS vaccinatiegegevens.* *"Hoewel de definitie zoals hierboven uiteengezet aangeeft dat het integriteitsniveau op Midden kan worden gezet voor genoemd proces en programmatuur, is gekozen voor Hoog. Dit komt doordat er vanuit een ander perspectief naar wordt gekeken. Gegevens in CIMS (vaccinatieregistratie) op persoonsniveau zijn dusdanig van belang voor direct betrokkene dat de juistheid, tijdigheid en volledigheid van vaccinatieregistratie op orde moeten zijn. Het heeft dus niet zozeer met politieke gevoeligheid of financiële gevolgen te maken als wel met de gevoeligheid van de gegevens op zich en de gevolgen als er sprake is van onjuiste weergave en niet-tijdige verwerking."* **Wij leveren een View op database, waarin niets gewijzigd kan worden. Integriteit is onderdeel van QuickScan van CIMS met beveiligingsmaatregelen op Integriteit van data.**
RIVMToegang *(Bron: Quickscan BIO RIVMToegang - v1.0)*	*M*	*ISO27001 gecertificeerde SaaS oplossing met Signicat. Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
COVID-19 vaccinatie Informatie- en Monitoringsysteem (CIMS).	*H*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
DigID	*M*	*Buiten scope voor deze QuickScan, want valt onder RIVMToegang.*
Interne API Manager	*M*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*

H	**Impactclassificatie voor vertrouwelijkheid**			
	Impact	**Imagoschade** *Publieke reputatie, vertrouwen*	**Financiële schade** *Additionele kosten*	**Uitval schade** *Operatie*
	Laag *Beperkte schade* *Ongerubriceerde informatie*	• Irritaties en ongemak burgers geventileerd in media • Negatieve publiciteit	• Op te vangen binnen de begroting van ministerie of XXXX	• Beperkt verlies van management control
	Midden *Forse schade* ***Te Beschermen Belangen** in processen van de Rijksdienst*	• Verlies van publiek respect • Klachten van burgers • Negatieve publiciteit Verlies aan motivatie medewerkers	• Niet op te vangen binnen de begroting van ministerie of XXXX • Accountantsverklaring niet afgegeven	• Belangrijk verlies van management control
	Hoog	• Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3 • Informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2) • Aansluiting op een infrastructuur vereist BBN3 om informatie te kunnen verwerken • Weerstand tegen statelijke actoren is noodzakelijk		

Informatie/systeem	Classificatie informatie *Laag, Midden, Hoog*	Toelichting
Cliëntportaal	*M*	*Clientportaal zelf bevat geen gegevens. Wij kijken daarom naar de dienst die ontsloten wordt: CIMS vaccinatiegegevens. Het gaat om medisch vertrouwelijke persoonsgegevens. Deze zijn op departementaal vertrouwelijk gesteld. Tevens is gekozen dat deze met DigID als authenticatiemiddel te ontsluiten moeten zijn, wat niet het zwaarste middel is.* **Geen risico op statelijke actoren.**
RIVMToegang *(Bron: Quickscan BIO RIVMToegang - v1.0)*	*M*	*ISO27001 gecertificeerde SaaS oplossing met Signicat.* *Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
CIMS - COVID-19 vaccinatie Informatie- en Monitoringsysteem.	*H*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*
DigID	*M*	*Buiten scope voor deze QuickScan, want valt onder RIVMToegang.*
Interne API Manager	*M*	*Buiten scope voor deze QuickScan, want heeft eigen QuickScan en RisicoAnalyse.*

STAP 4: Samenvatting Quickscan & resultaten vaststellen

I	**Samenvatting**											
	STAP 1		**STAP 2**				**STAP 3**					
	(X)	**Rubricering**	(X)	**Classificatie**	(X)	**Classificatie**	(X)	**B**	(X)	**I**	(X)	**V**

			proces		systeem						
	Openbaar		Ondersteunend	X	Nuttig		Laag		Laag		Laag
	XXXX Intern (besloten)	X	Bijdragend		Belangrijk		Midden	X	Midden	X	Midden
X	XXXX Vertrouwelijk		Strategisch		Vitaal	X	Hoog		Hoog		Hoog
	Departementaal Vertrouwelijk		Kritisch strategisch								
	Staatsgeheim Confidentieel										
	Staatsgeheim Geheim										
	Staatsgeheim Zeer Geheim										

J Resultaat

	Resultaat	Toelichting
BBN *1, 2, 3 of VIR-BI*	*BBN-2*	*Voor CliëntPortaal: BBN-2. Een hoger BBN niveau geeft extra eisen aan authenticatie en klant-onboarding. Voor aan te sluiten diensten die een zwaarder authenticatiemiddel eisen kunnen afzonderlijke afspraken gemaakt worden. In CliëntPortaal geen statelijke actoren die BBN3 vragen.*
RTO *5dgn, 2dgn of < 2dgn*	*<2dgn*	*Geen opmerking.*
RPO *28hr, 24hr of <24hr*	*Nvt*	*CliëntPortaal slaat zelf geen gegevens op.*
Externe eisen *NAVO, EU, ketenpartner, andere organisatie, AVG*	*EU, AVG, DigID assessment*	*Verwerkt AVG gevoelige gegevens; data binnen EU; DigID assessment vereist voor RIVMToegang. Zonder DIGID assessment is Cliëntportaal niet mogelijk. Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg – WABVPZ.*
Uitvoeren Risicoanalyse? *Ja of nee*	*Ja*	*Internetfacing, AVG data.*

Tekenformulier

- Op 15 februari (*) en 3 maart (**) 2021 heeft een workshop QuickScan Information Security plaatsgevonden voor Cliëntportaal met koppeling aan CIMS vaccinatiegegevens met ondersteunende informatiesystemen RIVMToegang, CIMS, DigID en API manager.
- Bij deze workshop waren aanwezig:

Naam	Functie	Afdeling
5.1.2e 5.1.2e (*)	- Infra	- SSC Campus,
5.1.2e 5.1.2e 5.1.2e (*)(**)	- Applicatiemanager / Key User	Basisinfrastructuur
	-	- SSC Campus Applicatie- en
5.1.2e 5.1.2e (*)	- Product Owner/ Accountmanager	functionaliteiten management
5.1.2e *)	RVP	- DVP
5.1.2e 5.1.2e (*)	- Applicatie en servicepunt	- SSC Campus
	- Applicatie en servicepunt,	- SSC Campus
5.1.2e 5.1.2e (*)(**)	Functioneel beheer	- SSC Campus
	- Projectmanager / Plaatsvervangend	-
5.1.2e 5.1.2e (*)(**)	- Eigenaar	- CIO Office
5.1.2e 5.1.2e (*)(**)	- Informatie manager	- CIO Office
5.1.2e 5.1.2e (*)(**)	- Adviseur Informatiebeveiliging	- CIO Office
	- Adviseur Informatiebeveiliging	-
	-	

- *Ik heb kennisgenomen van de inhoud van het rapport en stem in met de resultaten van deze QuickScan. De resultaten van de Quickscan zijn geldig tot het moment dat de gegevens waarop deze zijn gebaseerd wijzigen.*

BIJLAGE A: invullen van de Quickscan

ALGEMEEN	
Voor iedere tabel geldt dat de grijs gearceerde deel moeten worden ingevuld indien '(X)' wordt vermeld dient aangekruist te worden wat van toepassing is.	
STAP 1: Bepaal de scope, context en rubricering	
A	De scope kan uitgaan van een proces met één of meerdere ondersteunende systemen of één informatiesysteem dat meerdere processen ondersteunt. Geef in tabel A aan welke processen met ondersteunende systemen tot de scope van de analyse behoren.
B	Vul per proces, dat tot de scope behoort, tabel B in. Vallen meerdere processen onder de scope dan dient per proces een tabel B ingevuld te worden.
C	a. Vul per informatiesysteem, dat tot de scope behoort, tabel C in. Als er meerdere informatiesystemen onder de scope vallen dan dient per informatiesysteem een tabel C ingevuld te worden. b. Geef aan of het informatiesysteem gerubriceerde informatie verwerkt. Als er meerdere soorten informatie in de informatiesystemen worden verwerkt dan dient per informatiesoort het rubriceringsniveau te worden vermeld in de tabel c. Geef in tabel C per informatiesysteem aan welke eisen externe partijen daaraan stellen.
STAP 2: Classificeer proces en informatiesysteem en bepaal externe eisen	
D	Ieder proces wordt geclassificeerd naar de mate van belang. In tabel D worden de classificaties weergegeven. Kruis in tabel D aan welke classificatie voor het proces van toepassing is en geef onderaan een argumentatie voor de gemaakte keuze.
E	In onderstaande tabel is een overzicht gegeven van mogelijke classificaties van het informatiesysteem. De classificaties geven een waarde aan die men hecht aan het informatiesysteem ter ondersteuning van het proces. Vermeld het informatiesysteem achter de juiste classificatie in tabel E.
STAP 3: Bepaal betrouwbaarheidseisen	
F	Beschikbaarheid betreft het waarborgen, dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen) (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007). Geef *in tabel F aan of de impact 'Laag', 'Midden' of 'Hoog' is.* Geef tevens de argumentatie hiervoor in termen van: a. Beschrijf bijvoorbeeld de minimale eisen die gesteld worden aan de beschikbaarheid (ook in de piekperiodes). Komt dit overeen met de afgesloten SLA? b. Welke eisen worden gesteld aan bijvoorbeeld het weer beschikbaar hebben van de data bij verlies? c. Zijn er wettelijke termijnen die gehaald moeten worden? d. Zijn er contractuele verplichtingen qua beschikbaarheid afgesproken naar burgers? e. Zijn er politieke processen die een bepaalde beschikbaarheid/response tijdvereisen? f. Zijn er resultaten van andere quickscans die leiden tot hogerebeschikbaarheidseisen? g. Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden. h. Geef aan wat de Recovery Time Objective (de maximale benodigde hersteltijd) en i. Recovery Point Objective (maximaal toelaatbare hoeveelheid dataverlies) zijn.
G	Integriteit betreft het waarborgen van de juistheid en volledigheid van informatie en de verwerking ervan. De juistheid en volledigheid van de informatie is een directe verantwoordelijkheid van de eigenaar van het informatiesysteem en de hem ondersteunende managers en medewerkers (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007). Geef *in tabel G aan of de impact 'Laag', 'midden' of 'Hoog' is.* Geef tevens de argumentatie hiervoor in termen van: a. Beschrijf waarom welke integriteitseisen aan de informatie worden gesteld. b. Zijn er workarounds, is er bijvoorbeeld een papieren schaduwdossier, worden fouten snel herkend, wordt het vier ogen principe gehanteerd, wordt functiescheiding toegepast? c. Zijn er fouttoleranties afgesproken met burgers/afnemers? d. Zijn er resultaten van andere Quickscans die leiden tot hogere integriteitseisen? e. Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden.
H	Vertrouwelijkheid betreft het waarborgen dat informatie alleen toegankelijk is voor degenen, die hiertoe zijn geautoriseerd. Het gaat hier onder andere om het beveiligen van de toegang tot de

gebouwen, de informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, Trojaanse paarden). En het gaat ook om maatregelen om te voorkomen dat de eigen medewerkers toegang krijgen tot informatie die niet voor hen is bedoeld (uit: Voorschrift Informatiebeveiliging Rijksdienst 2007). Geef *in tabel H aan of de impact 'Laag, 'Midden' of 'Hoog' is.* Geef tevens de argumentatie hiervoor in termen van:

a. Beschrijf wat voor soort informatie in het proces en informatiesysteem wordt verwerkt. Is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie en welke belangen worden geschaad bij het openbaar worden van dezeinformatie?

a. Worden er wettelijke eisen aan de vertrouwelijkheid gesteld (bijv. AVG)?

a. Zijn er contractuele verplichtingen qua vertrouwelijkheid afgesproken naarburgers?

a. Zijn er resultaten van andere Quickscans die leiden tot hogere vertrouwelijkheidseisen?

a. Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden.

a. STAP 4: Samenvatting resultaten en vaststellen

a. l

a. Geef in tabel K een samenvatting van de resultaten uit de Quickscan.

b. Vermeld op basis het van de samenvatting:

a. het BNN-niveau. ***BBN3 niveau is van toepassing indien dreiging heerst vanuit statelijke actoren.***

b. RPO en RTO eisen

c. of er wel of niet aanvullend een risicoanalyse uitgevoerd moet worden. Neem bij twijfel hierover even contact op met de CISO.

d.

e. ***BBN2 te zwaar***:

- politieke schade aan een bewindspersoon: bewindspersoon moet voor verantwoording
- naar de Tweede Kamer, bijvoorbeeld n.a.v. Kamervragen; of
- diplomatieke schade te herstellen door ambtelijke opschaling; of
- financiële gevolgen; niet meer op te vangen binnen de begroting van het ministerie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of
- verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of
- bindende aanwijzing van de AP in verband met schending van de privacy; of
- directe imagoschade, bijvoorbeeld door negatievepubliciteit.

f. Zijn dergelijke schades niet aan de orde, dan is BBN1 van toepassing.

g.

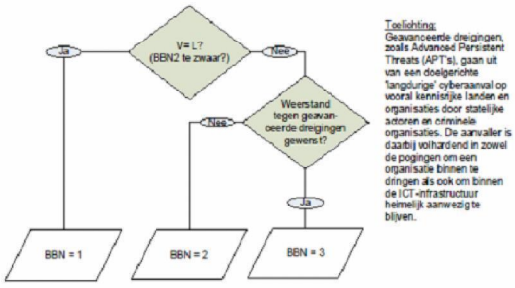
a. J

h. *BBN2 is onvoldoende indien*:

- de informatie beschermd dient te worden tegen statelijke actoren of vergelijkbare dreigers; of
- informatie wordt geleverd door derden en deze voor de beveiliging van betreffende informatie BBN3 eisen; of
- aansluiting op een infrastructuur het BBN3 vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen)

i. In elk van deze gevallen is BBN3 of hoger (zie VIR-BI) van toepassing.

j.



k.

l.

m.