Quickscan BIO RIVM

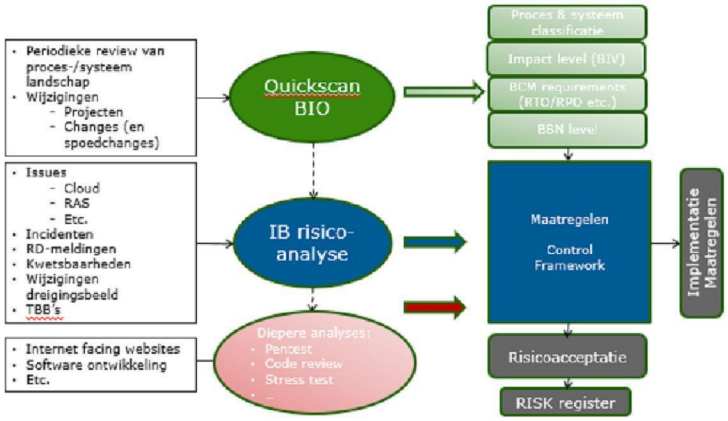
Kwalitatieve dataverzameling t.b.v. gedragsunit Corona en input OMT

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

		Uitvoeren interviews t.b.v. verkrijgen kwalitatieve en verdiepende data over gedrag.	***Aanvullend kwalitatief onderzoek onder migrantengroepen en laag geletterden***
		Er worden interviews afgenomen om verdiepende vragen te kunnen stellen op de online vragenlijst over corona en gedrag. Hier volgen factsheets uit die elke twee weken aan gedragsunit en OMT worden geleverd.	*Dit onderdeel wordt uitbesteed aan Pharos.*
Af	***Interviews worden telefonisch afgenomen. Bellen via mobiel en opname via ipad. Bellen twee devices (ipad en/of interne mensen).***	*Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces*	
	Map r- schijf	*De audiobestanden en het tekstbestand met de uitwerking van het interview worden opgeslagen in een projectmap met beperkte toegang.*	
	Uitwerking door Uitgetypt	*De audiobestanden van interviews worden geleverd aan Uitgetypt en de uitgewerkte tekstbestanden worden teruggestuurd naar het RIVM.*	
	Software Maxqda	*Software kwalitatief onderzoek*	

B	***Uitvoeren interviews t.b.v. verkrijgen kwalitatieve en verdiepende data over gedrag***
De klant van het proces	*De klant is degene die direct aan het eind van het proces het resultaat (de output) afneemt:* - *Interne klant: gedragsunit Corona. De gedragsunit levert vervolgens advies aan OMT.* - *Opdrachtgever is NWO.*
De output van het proces	*Op kort termijn 1 keer in de 2 weken een factsheets met impressies uit de interviews. Daarna wordt gestart met de volledige analyses van de internviews. Nog niet bekend hoe de output zal zijn.*
Koppelvlakken met andere processen	*Het is nog niet bekend of ook andere processen en/of projecten ook gebruik zullen gaan maken van de data.*
Gebruikte systemen	*De informatiesystemen die worden gebruikt bij de activiteiten in het proces:* - *telefonisch afname interviews en opnamen i-pad.* - *Map R-schijf* - *Uitwerking door Uitgetypt* - *Software Maxqda*

B	***Aanvullend kwalitatief onderzoek onder migrantengroepen en laag geletterden***
De klant van het proces	*De klant is degene die direct aan het eind van het proces het resultaat (de output) afneemt:* - *Uitvoerder: Pharos* - *Interne klant: gedragsunit Corona. De gedragsunit levert vervolgens advies aan OMT.* - *Opdrachtgever is NWO.*
De output van het proces	
Koppelvlakken met andere processen	*Het is nog niet bekend of ook andere processen en/of projecten ook gebruik zullen gaan maken van de data.*
Gebruikte systemen	*De informatiesystemen die worden gebruikt bij de activiteiten in het proces:* - Opdracht wordt in het geheel uitbesteed aan Pharos (er zal nagegaan worden welke beveiliging zet inzetten bij de uitvoering van het onderzoek)

C	***Telefonische afname van interviews***
Eigenaar informatiesysteem	*RIVM* – De devices die gebruikt worden zijn uitgegeven door SSC Campus.
De gebruikers van het informatiesysteem	*Degene die werkzaam zijn met het informatiesysteem* - *Intern: medewerkers RIVM (G&M /VPZ)* - *Extern: geen externe gebruikers*
De output van het informatiesysteem	Twee audio bestanden: 1: Toestemmingsverklaring voorgelezen en toestemming erop door geïnterviewden

		2: Interview Beide audiobestanden worden van het device verwijderd nadat ze op de R- schijf zijn geupload.
	Koppelvlakken met andere informatiesystemen	*Geen geautomatiseerde koppelingen aanwezig.*
	Andere processen	*Geen*
	Kritische momenten	*Dit onderzoek moet met grote snelheid worden uitgevoerd. Het levert inzicht voor de gedragsunit Corona en daarmee het OMT. De interviews worden tot half juli uitgevoerd.*
	Soort informatie	*Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt: privacygevoelige informatie en mogelijk politiek gevoelige informatie.*
	Data rubricering[1]	*RIVM vertrouwelijk*
	Externe eisen	*Geen bekende externe eisen*

C	***Map R-schijf***	
	Eigenaar informatiesysteem	*RIVM – G&M –* (10)(2e)
	De gebruikers van het informatiesysteem	*Degene die werkzaam zijn met het informatiesysteem:* - *Interne gebruikers: medewerkers RIVM die deel uitmaken van de projectgroep (meerdere centra bij RIVM).* - *Externe gebruikers: geen.*
	De output van het informatiesysteem	*Het betreft opslag van bestanden. De audiobestanden van*
	Koppelvlakken met andere informatiesystemen	*Geen geautomatiseerde koppelingen aanwezig*
	Andere processen	*Het is nu niet bekend of de uitgewerkte interviews voor andere onderzoeken/processen zullen worden gebruikt.*
	Kritische momenten	*Dit onderzoek moet met grote snelheid worden uitgevoerd. Het levert inzicht voor de gedragsunit Corona en daarmee het OMT. De interviews worden tot half juli uitgevoerd.*
	Soort informatie	*Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt: privacygevoelige informatie en mogelijk politiek gevoelige informatie.*
	Data rubricering[2]	*RIVM vertrouwelijk*
	Externe eisen	*Geen bekende externe eisen.*

C	***Uitwerking door Uitgetypt***	
	Eigenaar informatiesysteem	*uitgetypt*
	De gebruikers van het informatiesysteem	*Degene die werkzaam zijn met het informatiesysteem* - *RIVM: projectmedewerkers RIVM* - *Uitgetypt: zie beschrijving in document 'beschrijving bestanden delen met uitgetypt.*
	De output van het informatiesysteem	Tekstbestanden
	Koppelvlakken met andere informatiesystemen	*Data wordt geupload op het portaal van uitgetypt en de uitgewerkte tekstbestanden kunnen daar weer worden opgehaald. zie beschrijving in document 'beschrijving bestanden delen met uitgetypt.*
	Andere processen	*De processen van uitgetypt lopen via dit portaal.*
	Kritische momenten	*Dit onderzoek moet met grote snelheid worden uitgevoerd. Het levert inzicht voor de gedragsunit Corona en daarmee het OMT. De interviews worden tot half juli uitgevoerd.*
	Soort informatie	*Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt: privacygevoelige informatie en mogelijk politiek gevoelige informatie.*
	Data rubricering[3]	*RIVM vertrouwelijk*
	Externe eisen	*RIVM heeft als eis dat na goedkeuring van de tekstbestanden door het RIVM. Uitgetypt het audiobestand en het tekstbestand deleten. Dit moet ook gelden voor de back-up.*

C	***Software Maxqda***	
	Eigenaar informatiesysteem	*Maxqda is software waar het RIVM licenties voor afneemt.*
	De gebruikers van het informatiesysteem	*Degene die werkzaam zijn met het informatiesysteem* - *Interne gebruikers vanuit dit proces: medewerkers RIVM die deel uitmaken van de projectgroep (meerdere centra bij RIVM).*
	De output van het informatiesysteem	Kwantitatieve gegevens over kwalitatieve data.
	Koppelvlakken met andere informatiesystemen	*Geen geautomatiseerde koppelingen aanwezig*
	Andere processen	*Maxqda ondersteunt een groot aantal processen bij het RIVM waar kwalitatief onderzoek wordt uitgevoerd.*
	Kritische momenten	*Dit onderzoek zal zsm na uitwerking van de interviews maar naar verwachting ook na 11 juli plaatsvinden.*
	Soort informatie	*Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt: privacygevoelige informatie en*

[1] Zie ook *http://wiki.rivm.nl/inwiki/bin/view/Informatiebeveiliging/Classificatie+van+Informatie*
[2] Zie ook *http://wiki.rivm.nl/inwiki/bin/view/Informatiebeveiliging/Classificatie+van+Informatie*
[3] Zie ook *http://wiki.rivm.nl/inwiki/bin/view/Informatiebeveiliging/Classificatie+van+Informatie*

		mogelijk politiek gevoelige informatie.
	Data rubricering[4]	*RIVM vertrouwelijk*
	Externe eisen	*Geen bekende externe eisen.*

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**
Uitvoeren interviews t.b.v. verkrijgen kwalitatieve en verdiepende data over gedrag.	*Kritisch Strategisch*	*De output van dit proces wordt gebruikt door de gedragsunit Corona, dat advies geeft aan het OMT. Op basis van het advies van OMT worden maatregelen genomen in Nederland rond Corona. Dit proces is een van de processen die input leveren aan de gedragsunit maar kan in deze crisisperiode gezien worden als kritisch strategisch.*
Aanvullend kwalitatief onderzoek onder migrantengroepen en laag geletterden	*Kritisch Strategisch*	*De output van dit proces wordt gebruikt door de gedragsunit Corona, dat advies geeft aan het OMT. Op basis van het advies van OMT worden maatregelen genomen in Nederland rond Corona. Dit proces is een van de processen die input leveren aan de gedragsunit maar kan in deze crisisperiode gezien worden als kritisch strategisch*

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.

[4] Zie ook *http://wiki.rivm.nl/inwiki/bin/view/Informatiebeveiliging/Classificatie+van+Informatie*

	- Inzet van het informatiesysteem is essentieel voor een goede uitvoering van het bedrijfsproces.	
Informatiesysteemnaam	***Classificatie systeem N, B, V***	***Toelichting***
Interviews worden telefonisch afgenomen. Bellen via mobiel en opname via ipad. Bellen twee devices (ipad en/of Interne mensen).	*Belangrijk*	*De functie is vitaal maar het interview zou ook met andere soort devices kunnen worden afgenomen/opgenomen.*
Map r- schijf	*Belangrijk*	*De functie is vitaal maar het interview zou ook op andere wijze kunnen worden opgeslagen.*
Uitwerking door Uitgetypt	*Belangrijk*	*De functie is vitaal maar het interview zou ook op andere partij met inzet van ander systeem kunnen worden uitgewerkt.*
Software Maxqda	*Belangrijk*	*De functie is vitaal maar het interview zou ook met andere software kunnen worden geanalyseerd.*

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 RIVM	• 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 RIVM • 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**
Interviews worden telefonisch afgenomen. Bellen via mobiel en opname via ipad. Bellen twee devices (ipad en/of Interne mensen).	*Hoog*		*Als de audio bestanden verloren gaan voordat ze worden opgeslagen kunnen de factsheets die voor de gedragsunit worden gemaakt niet plaatsvinden.*
Map r- schijf	*Midden*		
Uitwerking door Uitgetypt	*Midden*		*Niet bekend welke dienstverlening ze hiervoor aanbieden.*
Software Maxqda	*Laag*	*Er zijn geen afspraken over RPO en RTO gemaakt.*	*Voor het doen van de analyses is meer tijd beschikbaar. Waardoor een lagere beschikbaarheide acceptabel is.*

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 RIVM	• 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 RIVM • 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
Interviews worden telefonisch afgenomen. Bellen via mobiel en opname via ipad. Bellen twee devices (ipad en/of Interne mensen).	*midden*	
Map r- schijf	*midden*	
Uitwerking door Uitgetypt	*midden*	*Omdat soms gesproken woord niet goed te verstaan is, wordt het uitgewerkte interview gecheckt door medewerker die het interview heeft afgenomen.*
Software Maxqda	*midden*	

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 RIVM	• Beperkt verlies van management control
Midden *Forse schade* ***Te Beschermen Belgngen 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 RIVM • 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
Interviews worden telefonisch afgenomen. Bellen via mobiel en opname via ipad. Bellen twee devices (ipad en/of Interne mensen).	*Midden*	*Als ergens in het proces vertrouwelijkheid wordt geschaad, zal de impact vrij hoog zijn in dit dossier waarbij er persoonsgegevens verzameld worden.*
Map r- schijf	*Midden*	*Als ergens in het proces vertrouwelijkheid wordt geschaad, zal de impact vrij hoog zijn in dit dossier waarbij er persoonsgegevens verzameld worden.*
Uitwerking door Uitgetypt	*Midden*	*Als ergens in het proces vertrouwelijkheid wordt geschaad, zal de impact vrij hoog zijn in dit dossier waarbij er persoonsgegevens verzameld worden.*
Software Maxqda	*Midden*	*Als ergens in het proces vertrouwelijkheid wordt geschaad, zal de impact vrij hoog zijn in dit dossier waarbij er persoonsgegevens verzameld worden.*

STAP 4: Samenvatting Quickscan & resultaten vaststellen

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	X	Belangrijk		Midden	X	Midden	X	Midden
X	RIVM Vertrouwelijk		Strategisch		Vitaal	X	Hoog		Hoog		Hoog
	Departementaal Vertrouwelijk	X	Kritisch strategisch								

		Staatsgeheim Confidentieel
		Staatsgeheim Geheim
		Staatsgeheim Zeer Geheim

J	Resultaat		
		Resultaat	**Toelichting**
	BBN *1, 2, 3 of VIR-BI*	*BBN2*	*Het betreft persoonsgegevens en hiermee gevoelige informatie die goed beschermt dient te worden. Het uitkomen van kwetsbaarheden*
	RTO *5dgn, 2dgn of < 2dgn*	*<2dgn*	*Er zit tijdsdruk op de uitvoering van dit onderzoek waardoor het van belang is dat alle informatiesystemen goed beschikbaar zijn.*
	RPO *28hr, 24hr of <24hr*	*<24 hr*	*Er zit tijdsdruk op de uitvoering van dit onderzoek waardoor het van belang is dat er geen data verloren gaat en dat geldt voornamelijk voor de oorspronkelijk audio bericht voordat deze is opgeslagen in systeem waar back-ups op plaatsvinden.*
	Externe eisen *NAVO, EU, ketenpartner, andere organisatie, AVG*	-	*Geen*
	Uitvoeren Risicoanalyse? *Ja of nee*	*Nee*	*Er wordt geen risicoanalyse geadviseerd gezien voor 3 van de 4 gebruikte systemen gebruik wordt gemaakt van standaard dienstverlening van het RIVM die geschikt is voor het doen van dit onderzoek en voor veel vergelijkbaar onderzoek wordt gebruikt. Een onderdeel wordt uitbesteedt en dit zal worden getoetst volgens de voorwaarden in verwerkingsovereenkomst.* *Er zijn nog wel een aantal aandachtspunten:* - *Veilige verzending van audiogegevens. Vanaf devices naar campus pro en naar/van uitgewerkt (toetsen van nader verstuurde informatie)* - *Nagaan of beschikbaarheid van de verschillende onderdelen kan worden gegarandeerd. Nagaan bij Uitbesteedt en Maxqda licenties.*

Tekenformulier

- Op 30 april 2020 heeft een workshop QuickScan Information Security plaatsgevonden voor Kwalitatieve dataverzameling t.b.v. gedragsunit Corona en input OMT met ondersteunende informatiesystemen telefonisch afname interviews en opnamen i-pad, Map R-schijf, Uitwerking door Uitgetypt en software Maxqda.

Bij deze workshop waren aanwezig:

Naam	Functie	Afdeling
(10)(2e)	*Eigenaar proces/systeem*	V&Z- KVZ
(10)(2e)	*Informatiemanager V&Z*	CIO-office

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 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? b. Worden er wettelijke eisen aan de vertrouwelijkheid gesteld (bijv. AVG)? c. Zijn er contractuele verplichtingen qua vertrouwelijkheid afgesproken naar burgers? d. Zijn er resultaten van andere Quickscans die leiden tot hogere vertrouwelijkheidseisen? e. Benoem hier ook de belangrijkste risico's/bedreigingen die gezien worden.
STAP 4: Samenvatting resultaten en vaststellen	
I	Geef in tabel K een samenvatting van de resultaten uit de Quickscan.
J	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.* ***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. Zijn dergelijke schades niet aan de orde, dan is BBN1 van toepassing. ***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) In elk van deze gevallen is BBN3 of hoger (zie VIR-BI) van toepassing.