Quickscan BIR RIVM

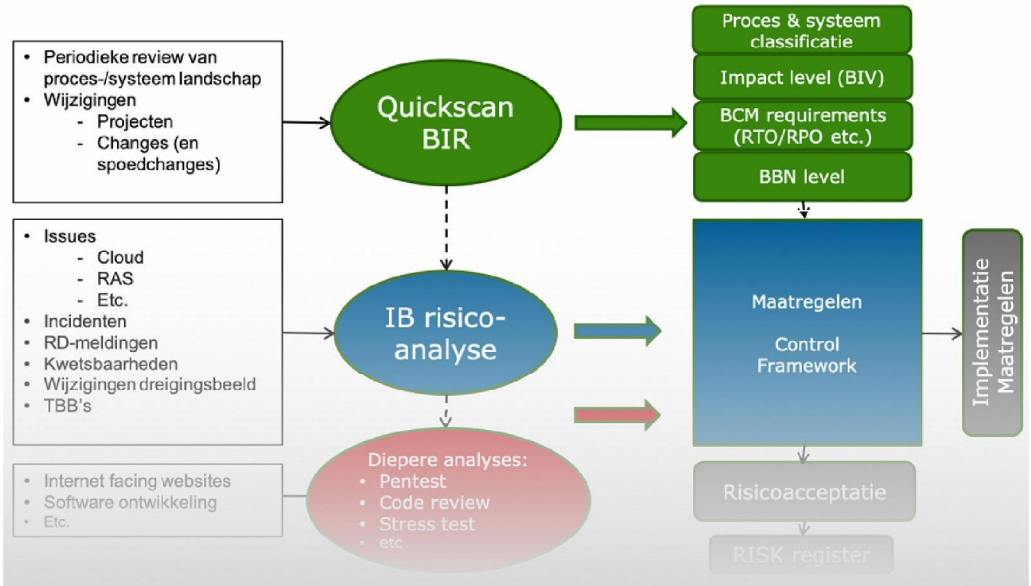
DVP bestelproces Covid19-vaccins en toebehoren

De quickscan Information Security (QIS), kortweg quickscan BIR, is het hulpmiddel om het basisbeveiligingsniveau (BBN) vast te stellen. Het is de BBN-toets zoals beschreven in de BIR2017. 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

		Bestellen van Covid19-vaccins en toebehoren	***Distribueren van Covid19-vaccins en toebehoren***
		Functionaliteit voor huisartsen, zorginstellingen, ziekenhuizen, arbodiensten en GGD'en om Covid19-vaccins en toebehoren (naalden, spuiten, oplosmiddel) te bestellen.	*Functionaliteit waarmee de vaste logistieke dienstverlener Movianto de bestelde goederen naar de regiokantoren van DVP of naar externe klanten kan distribueren.*
A	***SNPG Webapp***	*Huisartsen en een groot deel van de zorginstellingen plaatsen hun bestellingen via SNPG Webapp. Voor dit proces is een aparte quick scan uitgevoerd.* ***SNPG zal daarom verder buiten beschouwing gelaten worden in de voorliggende analyse.***	
	Formdesk	*Voor GGD'en vult DVP zelf de bestellingen op een Formdeskformulier in.* *Klanten die niet in SNPG zijn opgenomen, kunnen via Formdesk hun bestellingen plaatsen, waarna de gegevens weer in SAP worden ingelezen.* *Op termijn kunnen andere klanten hun bestelling direct in SAP-RIVM-DVP plaatsen.*	
	SAP-RIVM-DVP: ***-SAP/SD voor klantorder*** ***-SAP/MM voor voorraadbeheer***	*Bestelgegevens van klanten die opgenomen zijn in SNPG worden automatisch uit de SNPG Webapp in SAP gelezen.* *Bestelgegevens via Formdesk worden via import/export ingelezen in SAP-RIVM-DVP.*	
	SAP-Movianto		*Movianto krijgt de bestelgegevens in een beveiligde Zipfile via mail.* *De bestelling wordt uitgeleverd door Movianto.*

B1	***Bestellen van Covid19-vaccins en toebehoren***
De klant van het proces	- *Huisartsen, zorginstellingen, ziekenhuizen, arbodiensten, GGD'en*
De output van het proces	- *Een in SAP-RIVM-DVP geplaatste bestelling van het Covid19-vaccin en/of toebehoren met bepaalde omvang voor een specifieke klant.*
Koppelvlakken met andere processen	- *Voor huisartsen en deel zorginstellingen komt informatie uit SNPG Webapp* - *Resterende zorginstellingen of andere klanten niet in SNPG vullen Formdeskformulier in* - *Voor GGD'en vult DVP zelf een Formdeskformulier in* - *Op termijn kunnen andere klanten hun bestelling direct in SAP-RIVM-DVP plaatsen* - *Zet levering van vaccins en toebehoren door RIVM-DVP in gang via Movianto (SAP-Movianto)*
Gebruikte systemen	- *SNPG Webapp* - *Formdesk* - *SAP-RIVM-DVP*

B2	***Distribueren van Covid19-vaccins en toebehoren***
De klant van het proces	- *Huisartsen, zorginstellingen, ziekenhuizen, arbodiensten, GGD'en*
De output van het proces	- *Levering van bestelling bij specifieke klanten.*
Koppelvlakken met andere processen	- *SAP-RIVM-DVP* - *SAP Movianto.*
Gebruikte systemen	- *SAP-RIVM-DVP* - *SAP-Movianto* - *Zet levering van vaccins en toebehoren door Movianto in gang.*

C1	*SAP-RIVM-DVP*	
	Formdesk	
	Eigenaar informatiesysteem	*CIO-Office/FCC: proceseigenaar* 5.1.2e 5.1.2e
	De gebruikers van het informatiesysteem	*Medewerkers logistiek bij DVP, later mogelijk ook externe klanten*
	De output van het informatiesysteem	*Datafile om in te lezen in SAP-RIVM-DVP*
	Koppelvlakken met andere informatiesystemen	- SAP-RIVM-DVP - *Geen koppelvlak met CIMS*
	Andere processen	*N.v.t.*
	Kritische momenten	*Moet laatste week 2020 al beschikbaar zijn*
	Soort informatie	- *privacygevoelige informatie, commercieel vertrouwelijke informatie*
	Data rubricering[1]	*Departementaal Vertrouwelijk*
	Externe eisen	*AVG, Baseline Informatiebeveiliging Overheid (BIO)*

C2	*SAP-RIVM-DVP*	
	Eigenaar informatiesysteem	5.1.2e 5.1.2e 5.1.2e
	De gebruikers van het informatiesysteem	*Medewerkers logistiek bij DVP*
	De output van het informatiesysteem	*Bestelorder, afleverbon*
	Koppelvlakken met andere informatiesystemen	- *SNPG Webapp* - *Formdesk* - *SAP-Movianto (handmatig)* - *Geen koppelvlak met CIMS*
	Andere processen	*N.v.t.*
	Kritische momenten	*Snelle start per begin 2021.*
	Soort informatie	- *privacygevoelige informatie, commercieel vertrouwelijke informatie*
	Data rubricering[2]	*Departementaal Vertrouwelijk*
	Externe eisen	*AVG, Baseline Informatiebeveiliging Overheid (BIO)*

C3	*SAP-Movianto*	
	Eigenaar informatiesysteem	*Movianto*
	De gebruikers van het informatiesysteem	*Werknemers Movianto*
	De output van het informatiesysteem	*Bestelorder, afleverbon*
	Koppelvlakken met andere informatiesystemen	*N.v.t., krijgen gegevens via mail in beveiligde Zipfile*
	Andere processen	*N.v.t.*
	Kritische momenten	
	Soort informatie	- *privacygevoelige informatie*
	Data rubricering[3]	*Departementaal Vertrouwelijk*
	Externe eisen	*AVG, Baseline Informatiebeveiliging Overheid (BIO)*

[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*

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
Bestellen van Covid19-vaccins en toebehoren	*S*	*Zonder goed ingericht proces rond bestellen en distributie (inclusief voorraadbeheer) loopt het Covid19-vaccinatieprogramma direct schade op.*
Distribueren van Covid19-vaccins en toebehoren	*S*	*Zonder goed ingericht proces rond bestellen en distributie (inclusief voorraadbeheer) loopt het Covid19-vaccinatieprogramma direct schade op.*

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*
Formdesk	*V*	*Bestelformulier nodig om foutloos juiste hoeveelheden toebehoren te berekenen a.d.h.v. de bestelde hoeveelheid vaccin. Is back-up voor als niet alle zorginstellingen bestellen via de SNPG Webapp. Op termijn is dit de bestelwijze waarmee externe klanten bestellingen kunnen doen.*

SAP-RIVM-DVP	*V*	*De complete boekhouding rond bestellen, uitgifte en voorraadbeheer wordt door de desbetreffende modules in SAP ondersteund.*
SAP-Movianto	*V*	*Zonder deze SAP module kunnen de vaccins en toebehoren niet aan de klanten uitgeleverd worden.*

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**
Formdesk	*H*	*H*	*Bestelproces moet doorlopen om imagoschade te voorkomen*
SAP-RIVM-DVP	*H*	*H*	*Bestelproces moet doorlopen om imagoschade te voorkomen*
SAP-Movianto	*H*	*H*	*Bestelproces moet doorlopen om imagoschade te voorkomen*

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**
Formdesk	*H*	*Voor het verwerken van de bestelgegevens voor de Covid19-vaccins en toebehoren is er sprake van beschikbaarheid Hoog, aangezien zonder SAP de orders de deur niet uit kunnen waardoor landelijke vaccinatiecampagne in gevaar komt. Dit geldt gedurende het hele jaar.*
SAP-RIVM-DVP	*H*	*Voor het verwerken van de bestelgegevens voor de Covid19-vaccins en toebehoren is er sprake van beschikbaarheid Hoog, aangezien zonder SAP de orders de deur niet uit kunnen waardoor landelijke vaccinatiecampagne in gevaar komt. Dit geldt gedurende het hele jaar.*
SAP-Movianto	*H*	*Voor het verwerken van de bestelgegevens de Covid19-vaccins en toebehoren is er sprake van beschikbaarheid Hoog, aangezien zonder SAP de orders de deur niet uit kunnen waardoor landelijke vaccinatiecampagne in gevaar komt. Dit geldt gedurende het hele jaar.*

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 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 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
Formdesk	*H*	*Gegevens rondom vaccinvoorziening zijn vertrouwelijk van aard, zoals contracten (SNPG en Movianto) en prijzen.*
SAP-RIVM-DVP	*H*	*Gegevens rondom vaccinvoorziening zijn vertrouwelijk van aard, zoals contracten (SNPG en Movianto) en prijzen.*
SAP-Movianto	*H*	*Gegevens rondom vaccinvoorziening zijn vertrouwelijk van aard, zoals contracten (SNPG en Movianto) en prijzen.*

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		Belangrijk		Midden		Midden		Midden
		RIVM Vertrouwelijk	X	Strategisch	X	Vitaal	X	Hoog	X	Hoog	X	Hoog
	X	Departementaal Vertrouwelijk		Kritisch strategisch								
		Staatsgeheim Confidentieel										
		Staatsgeheim Geheim										
		Staatsgeheim Zeer Geheim										

J	Resultaat		
		Resultaat	**Toelichting**
	BBN *1, 2, 3 of VIR-BI*	*BBN3*	*Voor de Covid19-vaccinvoorziening geldt: commercieel vertrouwelijke informatie, leveranciersinformatie, grootschalige opslag, beheer en vervoer. Voor statelijke actoren of criminelen is het interessante informatie welke bestellingen/voorraden er waar zijn. Daarom wordt BBN3 als passend beschouwd.*
	RTO *5dgn, 2dgn of < 2dgn*	*< 2dgn*	*Bestelproces moet z.s.m. weer beschikbaar zijn.*
	RPO *28hr, 24hr of <24hr*	*< 24 hr*	*Levering vaccins moet z.s.m. weer doorgang vinden.*
	Externe eisen *NAVO, EU, ketenpartner, andere organisatie, AVG*	*AVG, BIO*	
	Uitvoeren Risicoanalyse? *Ja of nee*	*Ja*	

Tekenformulier

- Op 16 december 2020 heeft een workshop QuickScan Information Security plaatsgevonden voor DVP bestelproces Covid19-vaccins met ondersteunende informatiesystemen SAP-RIVM-DVP en SAP-Movianto.
-

- Bij deze workshop waren aanwezig:

Naam	Functie	Afdeling
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	[redacted]	
	[redacted]	
	-	-
		-
		-
		-
		-
		-
		-
		-

- *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 deze informatie?

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

a. Zijn er contractuele verplichtingen qua vertrouwelijkheid afgesproken naar burgers?

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

I

b. Vermeld op basis van de samenvatting in tabel J:

a. het BNN-niveau. ***BBN3 niveau is van toepassing indien er dreiging aanwezig is vanuit statelijke actoren of georganiseerde criminaliteit.***

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 negatieve publiciteit.

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

g.

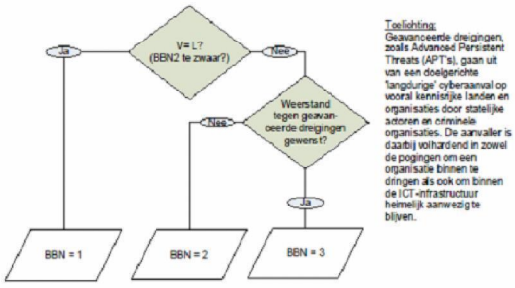
a. **J**

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.