

Quicksan BIO RIVM

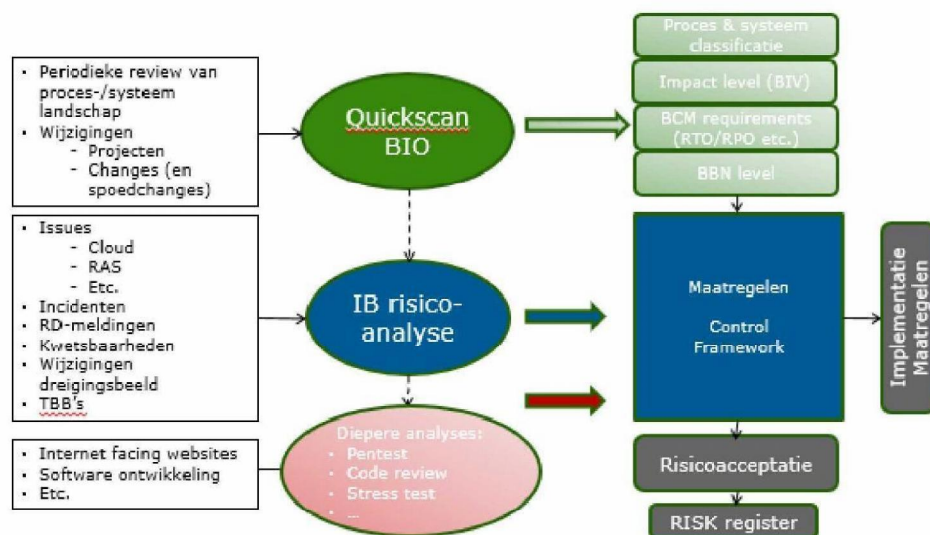
Monitoring determinanten COVID-19 vaccinatie: CIMS – CBS data aanlevering

De Quicksan Information Security (QIS), kortweg Quicksan 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 Quicksan 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

		Monitoring determinanten COVID-19 vaccinatie
		Zowel op landelijk als lokaal niveau en ook vanuit de politiek is er veel vraag naar inzicht in ontwikkelingen in de vaccinatiegraad en de betekenis voor de bescherming tegen COVID-19. Door middel van het koppelen van de vaccinatiegegevens uit CIMS en data tav sociaaleconomische, omgeving- en huishoud-determinanten van het CBS wordt hier meer inzicht in verkregen en kunnen meer gerichte maatregelen worden genomen om de vaccinatiegraad te verhogen door bijvoorbeeld voorlichtingscampagnes te organiseren bij groepen waar de vaccinatiegraad laag is. Het RIVM zal in nauwe samenwerking met VWS en CBS, statistische analyses en onderzoek gaan doen op de vaccinatiedata in combinatie met CBS microdata. Om de data te koppelen worden alle data gepseudonimiseerd in een beschermde omgeving van het CBS, door een speciaal ingericht en door de zogenoemde CBS-wet geautoriseerd team. Na pseudonimiseren is de data aan elkaar te koppelen door een unieke identificatiecode. Alleen geautoriseerde onderzoekers hebben toegang tot deze datasets en de data mag niet uit de beschermde omgeving worden gehaald. Alleen geaggregeerde data, waaruit geen persoon, instelling of vaccinfabrikant kan worden onthuld, mogen gepubliceerd worden en uit de CBS omgeving gehaald worden. De CBS vaccinatie data set zal beschikbaar worden gesteld via een RIVM SFTP server/directory bij het RIVM, die vervolgens door het CBS kan worden opgehaald. De CBS vaccinatie gegevens worden in het JSON formaat (UTF-8) aangeboden. Het CBS verkrijgt hiertoe een RIVM account waarmee zij toegang krijgen tot een RIVM SFTP server/directory. De JSON file zal worden gegenereerd vanuit de BI-CIMS omgeving, gezippt en vervolgens geplaatst worden op de backend SFTP server/directory. Het CBS vaccinatie bestand zal daarna beschikbaar worden gesteld op de front-end SFTP server, zodat deze kan worden opgepakt door het CBS. De bewaartermijn van het uiteindelijke CBS vaccinatie bestand en alle tussen bestanden zal steeds 48 uur bedragen.
A	CIMS	Vaccinatiedata als bron voor BI-CIMS Query.
	BI-CIMS	In BI-CIMS zal een query worden aangemaakt op grond van de specificaties in sectie Selectie criteria. De uitkomst van deze query - in JSON formaat - levert een tabelvormige dataset op die zal worden aangeboden op de SFTP locatie
	SFTP server back-end /front-end	De CBS vaccinatie data set zal beschikbaar worden gesteld via een SFTP server/directory bij het RIVM Het CBS verkrijgt hiertoe een RIVM account waarmee zij toegang krijgen tot een RIVM SFTP server/directory. (alleen op de front end van de server)
B	Monitoring determinanten COVID-19 vaccinatie	
	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 - <wie is de externe klant?> CBS, VWS
	De output van het proces	Onderzoeksresultaten Door middel van het koppelen van de vaccinatiegegevens uit CIMS en data tav sociaaleconomische, omgeving- en huishoud-determinanten van het CBS wordt hier meer inzicht in verkregen en kunnen meer gerichte maatregelen worden genomen om de vaccinatiegraad te verhogen door bijvoorbeeld voorlichtingscampagnes te organiseren bij groepen waar de vaccinatiegraad laag is.
	Koppelvlakken met andere processen	- Vaccinatie registratie - CBS
	Gebruikte systemen	De informatiesystemen die worden gebruikt bij de activiteiten in het proces: - BI-CIMS - SFTP server back end / front-end

BI-CIMS	
Eigenaar informatiesysteem	<naam van de eigenaar van het informatiesysteem> DVP-BIS, 5.1.2e
De gebruikers van het informatiesysteem	Degene die werkzaam zijn met het informatiesysteem - <wie is de interne gebruiker / klant?> RIVM medewerkers DVP - <wie is de externe gebruiker / klant?> n.v.t. - <aantal gebruikers / burgers> n.v.t.
De output van het informatiesysteem	Dataset vaccinatie gegevens.
Koppelvlakken met andere informatiesystemen	Len architectuurplaatje kan hier verhelderend werken.
	The diagram illustrates the architecture of the BI-CIMS system. It shows internal components such as 'Output Map' and 'Share' within the 'BI-CIMS SCOPE'. These are linked to external systems like 'RIVM' and 'CIMS'. A 'Top Deck Registratie' component is also shown. The diagram uses various icons and labels to represent different parts of the system and their interactions.
Andere processen	Welke andere processen worden door het informatiesysteem ondersteund? De data in BI-CIMS zal ook verwerkt worden om epidemiologische evaluaties te kunnen doen (fase vii). Doel van deze epidemiologische evaluatie is om het aantal gevaccineerden, de vaccinatiegraad, en de werking van het vaccin te bepalen. Rapportage over deze bevindingen vindt slechts op een geaggregeerd niveau plaats, waarbij er in redelijkheid geen sprake is van enige vorm van herleidbaarheid tot een betrokkene. Naast de periodieke (standaard) interne rapportages kunnen additionele rapportages worden gemaakt naar aanleiding van vragen van het ministerie van VWS, het Outbreak Management Team, de Gezondheidsraad. Verstrekking van deze informatie in het kader van rapportage over de vaccinatiecampagne aan de Minister van VWS, of via publieke rapportage, vindt plaats zonder herleidbare persoonsgegevens. In de uitvoering van epidemiologische evaluaties is voor wat betreft de bewaking en de evaluatie van het vaccinatieprogramma, het RIVM belast met de kwaliteitsbewaking door middel van: monitoring, centrale registratie en surveillance. Hiervoor wordt gebruik gemaakt van reeds geregistreerde gegevens in CIMS, welke in gepseudonimiseerde vorm in BI-CIMS worden verwerkt. Dit houdt onder meer het volgende in:
Kritische momenten	Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes. 1 keer per maand op vaste tijd vindt de aanlevering van data plaats.

SFTF server	5.1.2e 5.1.2e
Eigenaar informatiesysteem De gebruikers van het informatiesysteem	<i>Degene die werkzaam zijn met het informatiesysteem</i> - <wie is de interne gebruiker / klant?> RIVM medewerkers DVP - <i>wie is de externe gebruiker / klant?> CBS</i> - <i>aantal gebruikers: 10 personen voor dit proces, toegang alleen voor de voor dit proces gebruikte directory</i>
De output van het informatiesysteem Koppelvlakken met andere informatiesystemen	Databestand t.b.v. CBS en RIVM met (bijzondere) persoonsgegevens over vaccinatie. <i>Een architectuurplaatje kan hier verhelderend werken.</i>

4

	Andere processen	Welke andere processen worden door het informatiesysteem ondersteund? N.v.t.
	Kritische momenten	Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes. 1 maal per maand op vast tijdstip.
	Soort informatie	Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?) Persoonsgegevens en bijzondere persoonsgegevens • BSN Nummer • Geslacht • Geboortejaar • Vaccinnaam • Vaccinatie datum • Vaccinatiebatch • Toediener
	Data rubricering²	Welke classificatie is van toepassing op de informatie? (Openbaar, RIVM intern, RIVM 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 • Samenwerkingsovereenkomst met CBS • NEN7512

² 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 effectiviteits- 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 of uitvoeringsorganisatie. - 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 dit proces. 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
Monitoring determinanten COVID-19 vaccinatie		S
		het doel van dit proces is hoe de vaccinatiegraad te verhogen is

E	Classificatie van de informatiesystemen	
	Typering	Waardering
	Nuttig (N)	Het informatiesysteem geeft support bij de activiteiten binnen het 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 of diensten. - 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
BI-CIMS		B
SFTP server		B
		Er zijn andere manieren om het doel te bereiken
		Er zijn andere manieren om het doel te bereiken

STAP 3: Bepaal betrouwbaarheidseisen

F Impactclassificatie voor beschikbaarheid			
Impact	Imagoschade <i>Publieke reputatie, vertrouwen</i>	Financiële schade <i>Additionele kosten</i>	Uitval schade <i>Operatie</i>
Laag <i>RTO max. 5 dagen RPO max. 28 uur Beschikbaar 99%</i>	- Irritatie 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 <i>RTO max. 24 dagen RPO max. 24 uur Beschikbaar 99,5%</i>	- 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 <i>RTO <= 2 dagen RPO <= 24 uur Beschikbaar >= 99,9%</i>	- 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 <i>Laag, Midden, Hoog</i>	RPO & RTO	Toelichting
BI CIMS	L	5 dagen / 28 uur	Proces kan zo nodig opnieuw uitgevoerd worden.
SFTP server	L	5 dagen / 28 uur	Proces kan zo nodig opnieuw uitgevoerd worden.

G Impactclassificatie voor integriteit			
Impact	Imagoschade <i>Publieke reputatie, vertrouwen</i>	Financiële schade <i>Additionele kosten</i>	Uitval schade <i>Operatie</i>
Laag <i>Beperkte schade</i>	- Irritatie 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 <i>Forse schade</i>	- 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 <i>Laag, Midden, Hoog</i>	Toelichting	
BI CIMS	M	Onjuiste informatie/onderzoeksresultaten verstrekken aan VWS heeft rijksbrede negatieve publiciteit. Wel vinden er regelmatig correcties en controles plaats in BI CIMS. Iedere maand worden de gegevens opnieuw gestuurd, waardoor fouten kunnen worden ontdekt.	
SFTP server	M	Onjuiste informatie/onderzoeksresultaten verstrekken aan VWS heeft rijksbrede negatieve publiciteit.	

H Impactclassificatie voor vertrouwelijkheid			
Impact	Imagoschade <i>Publieke reputatie, vertrouwen</i>	Financiële schade <i>Additionele kosten</i>	Uitval schade <i>Operatie</i>
Laag <i>Beperkte schade Ongerubriceerde informatie</i>	- Irritatie en ongemak burgers geventileerd in media - Negatieve publiciteit	Op te vangen binnen de begroting van ministerie of RIVM	Beperkt verlies van management control
Midden <i>Forse schade Te Beschermen Belangen in processen van de Rijksdienst</i>	- 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 <i>Laag, Midden, Hoog</i>	Toelichting
BI CIMS	M	Verlies van publiek respect
SFTP server	M	Verlies van publiek respect

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	X	Laag		Laag		Laag
		RIVM Intern (besloten)		Bijdragend	X	Belangrijk		Midden	X	Midden	X	Midden
	X	RIVM Vertrouwelijk	X	Strategisch		Vitaal		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	BBN2	Betreft bijzondere persoonsgegevens
RTO 5dgn, 2dgn of < 2dgn	5	Proces kan zo nodig opnieuw uitgevoerd worden.
RPO 28hr, 24hr of < 24hr	28	Proces kan zo nodig opnieuw uitgevoerd worden.
Externe eisen NAVO, EU, ketenpartner, andere organisatie, AVG	AVG NEN7512	Overeenkomst CBS
Uitvoeren Risicoanalyse? Ja of nee	Ja	Combinatie van bijzondere persoonsgegevens / BBN 2 / NEN7512 Dreigingen in kaart brengen en retrisico's identificeren.

Tekenformulier		
Op 28-10-'21 heeft een workshop QuickScan Information Security plaatsgevonden voor ‘Monitoring determinanten COVID-19 vaccinatie: CIMS – CBS data aanlevering’ met ondersteunende informatiesystemen BI-CIMS en SFTP server.		
Bij deze workshop waren aanwezig / betrokken:		
Naam	Functie	Afdeling
5.1.2e (niet aanwezig)	5.1.2e	DVP-BIS
5.1.2e		EPI
5.1.2e		CIO-O
5.1.2e		EPI
5.1.2e		CBS
5.1.2e		DVP
5.1.2e		CIO-O
5.1.2e		EPI
5.1.2e		CIO-O
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 hogere beschikbaarheidseisen? 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 schaduw dossier, 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? 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. Vermeld op basis het van de samenvatting:
J	a. het BBN-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 negatieve publiciteit. 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.

