

Quickscan BIO RIVM

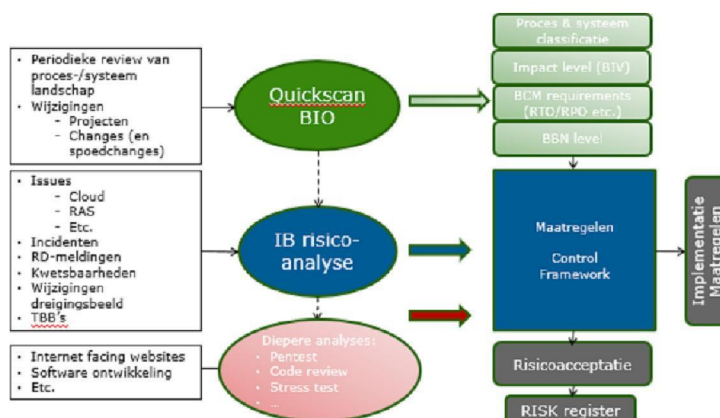
SNPG WebApp

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

		Bestellen vaccins	Bestellen informatie-materiaal	Declareren en melden vaccinaties
A	SNPG WebApp	Functionaliteit voor huisartsen en zorginstellingen om vaccins (griep, pneumokokken en evt. COVID-19) voor de doelgroepen te bestellen.	Functionaliteit voor huisartsen en zorginstellingen om informatiemateriaal voor cliënten te bestellen voor de genoemde vaccin-verstrekkingen.	Functionaliteit voor de huisartsen om de geplaatste vaccinaties te declareren en het aantal overgebleven vaccins en spillage door te geven. Functionaliteit voor de zorginstellingen om geplaatste vaccinaties, overgebleven vaccins en spillage door te geven.

B1	Bestellen vaccins
De klant van het proces	- Huisartsen en zorginstellingen zijn de gebruikers - SNPG is eigenaar van dit deelproces - RIVM-DVP is leverancier van de vaccins - RIVM-CvB is regievoerder
De output van het proces	- Een in SAP-RIVM-DVP geplaatste bestelling van een bepaald middel met bepaalde omvang voor een specifieke huisartsenpraktijk of zorginstelling.
Koppelvlakken met andere processen	- Geen aanleverende processen (handmatig door de huisartsenpraktijk/zorginstelling) - Zet levering van vaccins door RIVM-DVP in gang
Gebruikte systemen	- SNPG WebApp - Koppeling met SAP van RIVM-DVP

B2	Bestellen informatiemateriaal
De klant van het proces	- Huisartsen en zorginstellingen zijn de gebruikers - SNPG is eigenaar van dit deelproces - RIVM-CvB is regievoerder en verzorgt drukwerk aan verzendhuizen en koerier (RIVM is verantwoordelijk voor de inhoud, vormgeving en kwaliteit van de voorlichting en drukt daarom het materiaal af). - Xerox drukt voor het RIVM-CvB het informatiemateriaal af.
De output van het proces	- Bij SNPG komt een geplaatste bestelling van een bepaald voorlichtingsmiddel met bepaalde omvang voor een specifieke huisartsenpraktijk of zorginstelling.
Koppelvlakken met andere processen	- Geen aanleverende processen (handmatig door de huisartsenpraktijk/zorginstelling) - SNPG zet levering van informatiemateriaal in gang
Gebruikte systemen	- SNPG WebApp

B3	Declareren en melden vaccinaties
De klant van het proces	- Huisartsen en zorginstellingen zijn de gebruikers. - SNPG is eigenaar van dit deelproces. SNPG vergoedt de declaraties o.b.v. gelden uit de subsidieregeling. - Zorginstellingen krijgen vergoeding vanuit andere bron. - Het RIVM-CvB is regievoerder
De output van het proces	- Een in de SNPG WebApp geplaatste declaratie van een bepaalde vaccinatie en melding van overgebleven vaccin en spillage van bepaalde omvang voor een huisartsenpraktijk. Vernietiging van overgebleven vaccins ligt bij huisartsenpraktijken. - Een in de SNPG Webapp geplaatste melding van overgebleven vaccins en spillage van bepaalde omvang voor een specifieke zorginstelling. - Spillage en overgebleven vaccins wordt als XML output (in batch) met RIVM gedeeld.
Koppelvlakken met andere processen	- Geen aanleverende processen (handmatig door de huisartsenpraktijken) - Zet uitbetaling van SNPG aan huisartspraktijk in gang middels XML-output dat in een uitbetalingsapplicatie wordt ingelezen.
Gebruikte systemen	- SNPG WebApp

C	SNPG WebApp
Eigenaar informatiesysteem	- RIVM-CvB

De gebruikers van het informatiesysteem	- Huisartsen en zorginstellingen als eindgebruiker - SNPG verantwoordelijk voor onderhoud, functioneel beheer en doorontwikkeling. SNPG is tevens gebruiker van de applicatie - Direct ICT: hosting van applicatie - Partners 4 IT: onderhoud applicatie, functioneel beheer en doorontwikkeling
De output van het informatiesysteem	- Berichten voor bestellingen van vaccins naar RIVM-DVP-SAP. Met als resultaat dat huisartspraktijken en zorginstellingen worden voorzien van vaccins door RIVM DVP. - Huisartspraktijken en zorginstellingen ontvangen informatiemateriaal nadat bestelling bij SNPG is gedaan. - Huisartsenpraktijken ontvangen de vergoeding van de vaccinaties. - Er is inzicht in de overgebleven vaccins en spillage.
Koppelvlakken met andere informatiesystemen	- Koppeling voor orderberichten van vaccins met RIVM-DVP-SAP - Geen geautomatiseerde koppeling voor orderberichten informatiemateriaal, declaratieberichten en/of overgebleven vaccins richting RIVM of andere partijen. - Geen koppeling voor declaratie zorginstellingen; dit verloopt via andere financiering.
Andere processen	- Op dit moment niet. Er wordt onderzocht of onderdelen van dit systeem de COVID-19 vaccinatie zouden kunnen ondersteunen.
Kritische momenten	- Periode plaatsen bestellingen voor griep- en pneumokokkenvaccinatiecampagne (juni) - Tijdens griep- en pneumokokkenvaccinatiecampagne (september t/m december) - In december/ januari wanneer huisartsen declaraties indienen - Indien dit systeem wordt ingezet voor de COVID-19 vaccinatiecampagne dan komen er kritische momenten bij.
Soort informatie	De informatie die verwerkt wordt zijn NAW gegevens, bankrekeningnummers, AGB-codes en KVKnr's van de huisartsenpraktijken en zorginstellingen. Dit ten behoeve van bestelling en levering van materialen, alsmede het kunnen doen van betalingen aan huisartsenpraktijken. Bestelinformatie is kwetsbare informatie omdat daarmee te achterhalen is wanneer welke leveringen plaatsvinden. Deze leveringen zouden onderschept kunnen worden. In het licht van de COVID-19 vaccinatiecampagne zou bestelinformatie voor dlt vaccin politiek gevoelig kunnen zijn. Bijvoorbeeld omdat hoeveelheid aangevraagde/geleverde vaccins per doelgroep te herleiden is.
Data rubricering¹	RIVM vertrouwelijk. Zie informatie bij soort informatie.
Externe eisen	Geen externe eisen. Indien dit informatiesysteem gebruikt wordt voor de COVID-19 vaccinatie kunnen er externe eisen bijkomen zoals langere archiveer termijnen.

¹ Zie ook (10)(2g)

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 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	Toelichting
Bestellen vaccins	S	Proces is strategisch voor het kunnen uitvoeren van de vaccinatieprogramma's van de griep en pneumokokken. Dit deelproces wordt kritisch strategisch indien het gebruikt wordt voor het ondersteunen van de COVID-19 vaccinatie.
Bestellen informatiemateriaal	B	Ondersteunt de uitvoering van de griep en pneumokokken vaccinatieprogramma's.
Declareren en melden vaccinaties	B	Deelproces is belangrijk voor de continuïteit en draagvlak van de vaccinatieprogramma's.

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.	
	Vitaal (V)	- Het informatiesysteem wordt door veel (interne/externe) medewerkers/burgers gebruikt. - 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
SNPG WebApp		V	De applicatie ondersteunt in belangrijke mate de bedrijfsvoering van de vaccinatieprogramma's. SNPG WebApp zou vervangen kunnen worden

		door een ander geautomiseerd systeem. Automatisering is nodig in verband met nodig doorlooptijden en kritische momenten. Er zijn werkende work-arounds mogelijk, maar zeer arbeidsintensief.
--	--	--

STAP 3: Bepaal betrouwbaarheidseisen

F Impactclassificatie voor beschikbaarheid				
Impact	Imagoschade Publieke reputatie, vertrouwen	Financiële schade Additionele kosten	Uitval schade Operatie	
Laag <i>RTO max. 5 dagen RPO max. 28 uur Beschikbaar 99%</i>	- 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 <i>RTO max. 2 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 Laag, Midden, Hoog	RPO & RTO	Toelichting	
SNPG WebApp	L	<i>Hosting</i> RTO (Hersteltijd) prio 1 = 4 uur (binnen werktijden). RPO: maken van backups wel genoemd in SLA, maar niet de frequentie. <i>Technisch applicatiebeheer</i> Geen afspraken over RTO en/of RPO van de applicatie.	<i>Er zijn afzonderlijke contracten met de hostingpartij en voor het technisch applicatiebeheer en doorontwikkeling.</i> <i>Vermoedelijk is voor griep en pneumokokken de impactclassificatie Laag, maar met COVID-19 onder een nationaal vergrootglas zou ik Midden adviseren.</i>	

G Impactclassificatie voor integriteit				
Impact	Imagoschade Publieke reputatie, vertrouwen	Financiële schade Additionele kosten	Uitval schade Operatie	
Laag <i>Beperkte schade</i>	- 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 <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 Laag, Midden, Hoog	Toelichting		
SNPG WebApp	L	Voor de vaccinatieprogramma's griep en pneumokokken is de impactclassificatie Laag. Indien de applicatie ook gebruikt wordt voor COVID-19 dan zal de impact Midden worden.		

H Impactclassificatie voor vertrouwelijkheid				
Impact	Imagoschade Publieke reputatie, vertrouwen	Financiële schade Additionele kosten	Uitval schade Operatie	
Laag <i>Beperkte schade Ongerubriceerde informatie</i>	- 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	Verlies van publiek respect	Niet op te vangen binnen de	Belangrijk verlies van	

	<i>Forse schade</i> Te Beschermen Belangen in processen van de Rijksdienst	• Klachten van burgers • Negatieve publiciteit • Verlies aan motivatie medewerkers	• Accountantsverklaring niet afgegeven	
	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	
	SNPG WebApp	M	<i>Op Midden ingezet in verband met de soort informatie in het systeem en risico op onderschepping als onbevoegden in het systeem zouden kunnen.</i> <i>Indien het systeem wordt ingezet voor de COVID-19 vaccinatie dan zal de classificatie waarschijnlijk naar Hoog gaan.</i>	

STAP 4: Samenvatting Quicksan & resultaten vaststellen

I Samenvatting									
STAP 1		STAP 2			STAP 3				
Rubricering		Classificatie proces		Classificatie systeem		B		I	V
Openbaar		Ondersteunend		Nuttig	X	Laag	X	Laag	Laag
RIVM Intern (besloten)		Bijdragend		Belangrijk		Midden		Midden	X Midden
X RIVM Vertrouwelijk	X	Strategisch	X	Vitaal		Hoog		Hoog	Hoog
Departementaal Vertrouwelijk		Kritisch strategisch							
Staatsgeheim Confidentieel									
Staatsgeheim Geheim									
Staatsgeheim Zeer Geheim									

J Resultaat			
Resultaat	Resultaat	Toelichting	
BBN 1, 2, 3 of VIR-BI	BBN2	Voor de inzet van de SNPG WebApp ten behoeve van de griep en pneumokokkenvaccinatie is BBN2 voldoende. Indien deze Web applicatie ingezet ter ondersteuning van de COVID-19 vaccinatie dan zou het niveau wellicht naar BBN3 moeten gaan.	
RTO 5dgn, 2dgn of < 2dgn	5dgn (acceptabel)	Hosting: RTO (Hersteltijd) prio 1 = 4 uur (binnen werktijden).	
RPO 28hr, 24hr of <24hr	28 hr	Er zijn hier geen afspraken over gemaakt. Het is onbekend met welke frequentie back-ups worden gemaakt.	
Externe eisen NAVO, EU, ketenpartner, andere organisatie, AVG	Geen		
Uitvoeren Risicoanalyse? Ja of nee	Ja	Gezien het een web applicatie betreft dat vitaal is voor een tweetal vaccinaties is het noodzakelijk om een risicoanalyse uit te voeren en na te gaan of de tot nu toe genomen maatregelen voldoende zijn voor de gestelde eisen en classificatie. Aanvullend hierop wordt nu gekeken of dit systeem ook ingezet kan worden ter ondersteuning van de COVID-19 vaccinatie.	

Tekenformulier		
Op 6 oktober 2020 heeft een workshop QuickScan Information Security plaatsgevonden voor het bestellen van vaccins en informatiemateriaal en declareren en melden van vaccinaties met het ondersteunende informatiesysteem SNPG WebApp.		
Bij deze workshop waren aanwezig:		
Naam	Functie	Afdeling
(10)(2e)	Informatiemanager Domein V&Z	IV-organisatie
(10)(2e)	Programmamanager	CvB
(10)(2e)	Adviseur informatiemanagement	CvB
Met inhoudelijk bijdrage van het SNPG.		
<i>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.</i>		

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 tijd vereisen? 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 schaduwdoosier, 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: a. het BNN-niveau. BBN3 niveau is van toepassing indien dreiging heerst vanuit statelijke actoren. b. <i>RPO en RTO eisen</i> c. <i>of er wel of niet aanvullend een risicoanalyse uitgevoerd moet worden. Neem bij twijfel hierover even contact op met de CISO.</i> 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 imago schade, bijvoorbeeld door negatieve publiciteit. Zijn dergelijke schade niet aan de orde, dan is BBN1 van toepassing.
J	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. <pre> graph TD Q1{Is L7 (BBN2 te zwaar?)} -- Ja --> B1[BBN = 1] Q1 -- Nee --> Q2{Weerstand tegen geavanceerde dreigingen?} Q2 -- Ja --> B2[BBN = 2] Q2 -- Nee --> B3[BBN = 3] </pre> Geavanceerde dreigingen: Geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), gaan uit van een doelgerichte 'langdurige' of herhaalde opvoort aanval op land en organisaties door statelijke actoren en criminele organisaties. De aanval is doeltreffend en kan de ICT-infrastructuur ernstig aantasten.