Quickscan BIO RIVM

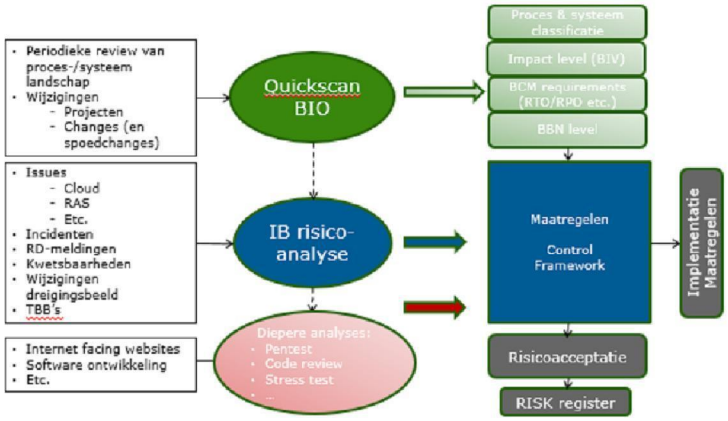
Diagnostiek COVID-19 in opdracht van GGD Amsterdam

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.



29 Mei 2020 V 0.1

STAP 1: Bepaal scope, context en rubricering

		Diagnostiek COVID-19 in opdracht van GGD Amsterdam	
		Gedurende de uitbraak van COVID-19 voert RIVM testen uit als MML en stuurt de resultaten terug naar het systeem CoronIT van de GGDen.	
A	***Unilab***	Unilab ontvangt de order voor een COVID-19 test via een HL7-bericht vanuit CoronIT. En stuurt het resultaat in een bulkbestand terug naar CoronIT.	
A	***BioNumerics***	Het monster wordt geanalyseerd mbv PCR techniek (Lightcycler technologie), de resultaten worden verwerkt in Bionumerics.	

B	***Diagnostiek COVID-19 in opdracht van GGD Amsterdam***	
	De klant van het proces	- *De persoon die zich laat testen* - *GGD Amsterdam*
	De output van het proces	*Uitslag van de test*
	Koppelvlakken met andere processen	*Met de geanonimiseerde data wordt nader onderzoek gedaan.*
	Gebruikte systemen	Unilab, Bionumerics

<Ingeval van meerdere processen kopieer blok B>

C	**Unilab**	
	Eigenaar informatiesysteem	IDS, (10)(2e)
	De gebruikers van het informatiesysteem	- *Medewerkers IDS* - *Functioneel beheer Unilab*
	De output van het informatiesysteem	De uitslag van de COVID-19 test
	Koppelvlakken met andere informatiesystemen	*Bionumerics*
	Andere processen	-
	Kritische momenten	*Tijdens een uitbraak*
	Soort informatie	- *Persoonsnummer* - *BSN* - *Patiënt naam* - *Geboortedatum* - *Geslacht* - *Adres patiënt* - *Ordernummer* - *Datum/tijd monsterafname* - *Materiaaltype* - *Arts (dummy naam)* - *Monsternummer* - *Herkomst materiaal* - *Beschrijving materiaal* - *Uitslag test*
	Data rubricering[1]	*RIVM vertrouwelijk*
	Externe eisen	*AVG, BIO*

<Ingeval van meerdere informatiesystemen kopieer blok C>

C	**Bionumerics**	
	Eigenaar informatiesysteem	IDS, (10)(2e)
	De gebruikers van het informatiesysteem	- *Medewerkers IDS*
	De output van het	

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

Koppelvlakken met andere informatiesystemen	- Unilab
Andere processen	
Kritische momenten	*Tijdens een uitbraak*
Soort informatie	Moleculaire data
Data rubricering[2]	*RIVM vertrouwelijk*
Externe eisen	*BIO, AVG*

<Ingeval van meerdere informatiesystemen kopieer blok C>

[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 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**
Diagnostiek COVID-19 in opdracht van GGD Amsterdam	*S*	*Deze taak is een van de vele taken van IDS/RIVM. Tijdens de uitbraak van COVID-19 is dit een kritisch proces, maar het RIVM voert hoofdzakelijk deze taak uit bij een grote uitbraak extra veel getest moet worden. Als dit proces stilvalt i heeft dit impact op de testcapaciteit voor de regio GGD Amsterdam (en in brede zin van Nederland). Het belangrijkste effect is dat de doorlooptijd van testen op loopt. Er is daarbij hooguit beperkte schade voor patiënt/volksgezondheid en geen groot risico op imagoschade bij RIVM/ Ministerie.*

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***

Unilab	*V*	*Het informatiesysteem is essentieel voor de uitvoering van het proces.*
Bionumerics	*V*	*Het informatiesysteem is essentieel voor de uitvoering van het proces.*

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**
Unilab	*Hoog*	*2 dagen, 24 uur*	*Risico op negatieve publiciteit en extra belasting van de organisatie bij uitval. Geen risico t.a.v. financiële schade. Beschikbaarheid en prioriteit is van belang. Risico op de schade aan imago loopt wel op na 2 dagen uitval van het systeem. Organisatie dient zsm te handelen om verstoringen te verhelpen.*
Bionumerics	*Hoog*	*2 dagen, 24 uur*	*Risico op negatieve publiciteit en extra belasting van de organisatie bij uitval. Geen risico t.a.v. financiële schade. Beschikbaarheid en prioriteit is van belang. Risico op de schade aan imago loopt wel op na 2 dagen uitval van het systeem. Organisatie dient zsm te handelen om verstoringen te verhelpen.*

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**
Unilab	*Midden*	*Risico op negatieve publiciteit en extra belasting van de organisatie bij uitval. Geen risico t.a.v. financiële schade.*

Bionumerics	*Hoog*	*Systeem is essentieel voor de continuïteit van het proces, er is geen alternatieve werkwijze.*

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**
Unilab	*Midden*	*Risico op imagoschade RIVM is groot. Wel sprake van verwerking persoonsgegevens. Gegevens hebben geen hoge, vertrouwelijk classificatie.*
Bionumerics	*Midden*	

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

J Resultaat

	Resultaat	Toelichting
BBN *1, 2, 3 of VIR-BI*	*2 dagen*	
RTO *5dgn, 2dgn of < 2dgn*	*2 dagen*	
RPO *28hr, 24hr of <24hr*	*24 uur*	
Externe eisen *NAVO, EU, ketenpartner, andere organisatie, AVG*	*AVG, BIO*	
Uitvoeren Risicoanalyse? *Ja of nee*	*Ja*	

Tekenformulier

Op 29 Juni 2020 heeft een workshop QuickScan Information Security plaatsgevonden voor het proces Diagnostiek COVID-19 in opdracht van GGD Amsterdam met ondersteunende informatiesystemen Unilab en Bionumerics.

Bij deze workshop waren aanwezig:

Naam	Functie	Afdeling
(10)(2e) (10)(2e)	(10)(2e)	Centrum IDS 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.