

Quickscan BIO RIVM

Online vragenlijst

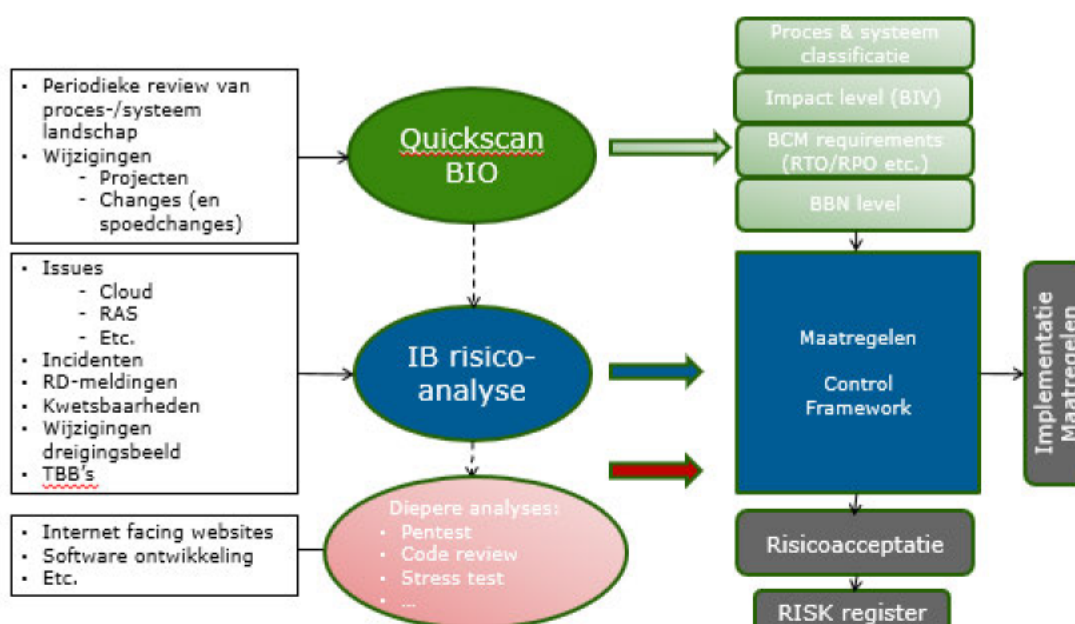
Gezondheidsmonitor Jeugd 2023

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

		Online vragenlijst Gezondheidsmonitor Jeugd 2023
		<i>Korte beschrijving van het proces</i> Dataverzameling: het afnemen van een vragenlijst voor de Gezondheidsmonitor (GM) Jeugd 2023 onder leerlingen van klas 2 en klas 4 op het regulier voortgezet onderwijs (ca. 200.000 scholieren). De vragenlijsten bevatten onderwerpen als social media gebruik, gamen, somatisch onvoldoende verklaarde klachten, et cetera. De vragenlijsten zijn vanaf half september 2023 in de lucht en de dataverzameling loopt tot eind november 2023. Het RIVM verzorgt de landelijke opschoning. De afdeling SIM van het RIVM maakt weegfactoren aan. Dit proces is onderdeel van het volgende meer overkoepelende deelproces van het centrum VPZ: "Dataverzameling (kwantitatief en kwalitatief) t.b.v onderzoek en evaluatie op het gebied van gezondheid, preventie en zorg".
A	Survalyzer Nederland BV	<i>Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces</i> Enquêtesoftware voor marktonderzoekers en bedrijven. Samen met de GGD'en heeft het RIVM een dienstverleningsovereenkomst afgesloten met verwerker Research 2Evolve. Deze externe partij is ingehuurd om de technische afname van digitale vragenlijsten mogelijk te maken d.m.v. software en tijdelijke dataopslag. Research 2Evolve gebruikt de enquêtesoftware van subverwerker Survalyzer Nederland BV. Research 2Evolve zorgt dat de vragenlijsten door leerlingen van klas 2 en klas 4 op het regulier voortgezet onderwijs kunnen worden ingevuld, worden opgeslagen en beschikbaar worden gesteld aan de GGD'en en het RIVM. Per school wordt een URL naar de vragenlijst uitgegeven door de bijbehorende GGD. Dit systeem wordt niet gebruikt door het RIVM, maar hierbij begint het ketenproces wel.
	Smartlockr	<i>Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces</i> Platform voor beveiligde bestandsuitwisseling. Voor versleutelde verzending en versleutelde toegang van datasets. Research 2Evolve zorgt dat na afloop van de dataverzameling (eind november 2023) iedere GGD het databestand van de eigen regio (basisvraagstellingen + lokale vraagstellingen) en dat het RIVM ook van alle GGD'en het databestand (enkel de basisvraagstellingen) ontvangt. Research 2Evolve stelt deze datasets ter beschikking via het platform SmartLockr. Daarvoor stelt Research 2Evolve inlogcodes ter beschikking aan daarvoor aangewezen medewerkers van de GGD'en en het RIVM welke vervolgens de databestanden kunnen downloaden van het platform. Hiertoe hebben alle GGD'en en het RIVM afzonderlijk met Research 2Evolve een verwerkingsovereenkomst afgesloten. GGD'en gaan vervolgens aan de slag met hun eigen databestand om (ongewogen) schoolprofielen te maken. Het RIVM krijgt dus alle databestanden en verzorgt dan de opschoning en weging. <i>Het RIVM is geen eigenaar van dit systeem, dat is Research 2Evolve. Wij kunnen gebruik maken voor de datatransactie</i>
	RIVM R-schijf	<i>Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces</i> Bij het RIVM worden de databestanden op de R-schijf opgeslagen. Alleen 4 leden van het projectteam hebben toegang tot ruwe data in de betreffende map (is gecontroleerd). Dit gaat specifiek om de map met databeheer.
	RIVM Filesender	<i>Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces</i> Het RIVM zorgt ervoor dat de databestanden van alle GGD'en worden opgeschoond en samengevoegd tot een landelijk bestand. Vervolgens verzorgt de afdeling SIM van het RIVM het aanmaken van een landelijke en gemeentelijke weegfactor. Eind februari 2024 ontvangen alle GGD'en hun eigen databestand (basisvraagstellingen + aangemaakte weegfactoren) en een geaggregeerde versie van het landelijk bestand van het RIVM via RIVM Filesender. GGD GHOR Nederland ontvangt ook een geaggregeerde versie van het landelijke databestand van het RIVM via RIVM Filesender.
	RIVM StatLine + VZinfo	<i>Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces</i> Resultaten van de Gezondheidsmonitor Jeugd 2023 worden gepresenteerd op RIVM StatLine en VZinfo.
	Digital Research Environment (DRE)	<i>Beschrijving van de ondersteunende functie van het informatiesysteem voor het proces.</i>

	In de Digital Research Environment van het RIVM wordt de data beschikbaar gesteld voor derden die onderzoek willen doen met de data uit de Gezondheidsmonitor Jeugd. Zo blijft RIVM eigenaar over de data.
--	--

B	Online vragenlijst Gezondheidsmonitor Jeugd 2023	
	De klant van het proces	<i>De klant is degene die direct aan het eind van het proces het resultaat (de output) afneemt:</i> - Interne gebruiker/klant van het proces: GGD'en en RIVM, zij ontvangen data van Research 2Evolve. - Externe gebruiker/klant van het proces: GGD'en en GGD GHOR Nederland, opdrachtgever VWS, beleidsmakers
	De output van het proces	<i>De output is het resultaat van handelen in het proces</i> Landelijk databestand met vragenlijstgegevens Gezondheidsmonitor Jeugd 2023 dat inzicht geeft in prevalentiecijfers van gezondheid, welzijn en leefstijl onder jeugd, zowel op landelijk en regionaal als gemeentelijk niveau.
	Koppelvlakken met andere processen	- <i>aanleverende processen/organisaties:</i> Research 2Evolve - <i>afnemende processen/organisaties:</i> RIVM, GGD'en, GGD GHOR Nederland, Gezondheidsonderzoek COVID-19
	Gebruikte systemen	<i>De informatiesystemen die worden gebruikt bij de activiteiten in het proces:</i> - Survalyzer Nederland BV - Smartlockr - RIVM R-schijf - RIVM Filesender (generiek RIVM-systeem, dus in de volgende blokken niet nader gespecificeerd) - RIVM StatLine (generiek RIVM-systeem, dus in de volgende blokken niet nader gespecificeerd) - DRE

<Ingeval van meerdere processen kopieer blok B>

C1	Survalyzer Nederland BV (wordt niet binnen RIVM gebruikt)	
	Eigenaar informatiesysteem	Research 2Evolve (neemt licenties af / heeft een contract met de leverancier)
	De gebruikers van het informatiesysteem	<i>Degene die werkzaam zijn met het informatiesysteem</i> - Interne gebruiker / klant: Research 2Evolve - Externe gebruiker / klant: scholen / scholieren (ca. 200.000). Per school wordt een URL uitgegeven - Aantal gebruikers: onbekend
	De output van het informatiesysteem	Dataverzameling. Ingevulde vragenlijsten.
	Koppelvlakken met andere informatiesystemen	Vanuit Survalyzer Nederland BV wordt de data gedownload door Research 2Evolve, zij versturen de data via Smartlocker naar GGD'en en RIVM.
	Andere processen	<i>Welke andere processen worden door het informatiesysteem ondersteund?</i> Bij het RIVM niet voor andere processen. Bij GGD onbekend. Niet bekend en niet relevant. Wij zijn geen eigenaar en maken ook geen gebruik.
	Kritische momenten	<i>Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes.</i> Een kritisch moment kan zijn wanneer er net communicatie uit is over het invullen. Dit verschilt heel erg per GGD, dus hier is geen specifiek moment aan te knopen. Het RIVM heeft hier niet goed zicht op. Tegen het einde van de looptijd (eind november) kan nog wel een laatste piek worden verwacht.
	Soort informatie	<i>Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?)</i> Er wordt privacygevoelige informatie verzameld. Deze is niet direct herleidbaar, mogelijk wel indirect. Er worden geen namen verzameld, maar wel leeftijd, geslacht en postcode 4. Soort gegevens: vragenlijsten met antwoorden met mogelijk (herleidbare) gewone en medische gegevens. De vragenlijsten bevatten namelijk een aantal gevoelige onderwerpen die iets zeggen over iemands gezondheid. Lijst met onderwerpen waarover vragen worden gesteld: - Opleiding - Leeftijd - Gender

	- Geografische indicator - Gezinssamenstelling - Moeite met rondkomen - Ervaren gezondheid - Geluk - Psychische klachten - Veerkracht - Eenzaamheid - Jonge mantelzorger - Functioneren op school - Bewegen - Stress - Prestatiedruk - Pesten - Sexting - Alcohol - Roken - Wiet en hasj - Sociale steun - Weerbaarheid - Suicidegedachten - Social media - Gamers
Data rubricering¹	<i>Welke classificatie is van toepassing op de informatie?</i> RIVM vertrouwelijk
Externe eisen	<i>Denk hierbij aan eisen vanuit de AVG, NAVO, EU, ketenpartner(s) en evt. andere organisatie(s).</i> AVG is van toepassing i.v.m. privacygevoelige informatie. Kan je hier ook uitleggen wat privacy gevoelig is?

C2	Smartlockr
Eigenaar informatiesysteem	Research 2Evolve (neemt licenties af / heeft een contract met leverancier). RIVM is geen eigenaar, maar een gebruiker.
De gebruikers van het informatiesysteem	<i>Degene die werkzaam zijn met het informatiesysteem</i> - Interne gebruiker / klant: Research 2Evolve - Externe gebruiker / klant: RIVM en GGD'en - Aantal gebruikers: naast gebruikers bij Research 2Evolve gaat het om enkele aangewezen personen bij het RIVM en bij GGD'en. 2 personen binnen het RIVM.
De output van het informatiesysteem	Databestanden met antwoorden op vragenlijsten: .sav bestanden.
Koppelvlakken met andere informatiesystemen	Vanuit Survalyzer Nederland BV wordt de data gedownload door Research 2Evolve, zij versturen de data via Smartlocker naar GGD'en en RIVM.
Andere processen	<i>Welke andere processen worden door het informatiesysteem ondersteund?</i> Niet bekend en niet relevant, het RIVM is gebruiker en geen eigenaar.
Kritische momenten	<i>Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes.</i> De momenten waarop Research 2Evolve de databestanden deelt met de externe gebruikers. Research 2Evolve deelt halverwege de dataverzameling de tussentijdse regionale bestanden van vijf GGD-regio's met het RIVM. Na afloop van de dataverzameling worden 26 regionale bestanden van GGD-regio's opgeleverd aan het RIVM.
Soort informatie	<i>Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?)</i> Privacygevoelige informatie. Zie ook de toelichting bij Survalyzer Nederland BV.
Data rubricering²	<i>Welke classificatie is van toepassing op de informatie?</i> RIVM vertrouwelijk

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>

	Externe eisen	<i>Denk hierbij aan eisen vanuit de AVG, NAVO, EU, ketenpartner(s) en evt. andere organisatie(s).</i> AVG is van toepassing i.v.m. privacygevoelige informatie.
--	----------------------	--

C3	RIVM Filesender met wachtwoord	
	Eigenaar informatiesysteem	IV-organisatie
	De gebruikers van het informatiesysteem	<i>Degene die werkzaam zijn met het informatiesysteem</i> - Interne gebruiker / klant: RIVM - Externe gebruiker / klant: GGD'en en GGD GHOR Nederland - Aantal gebruikers: 2 personen binnen het RIVM. Enkele aangewezen personen bij het GGD'en en GGD GHOR Nederland.
	De output van het informatiesysteem	Databestanden: .sav bestanden
	Koppelvlakken met andere informatiesystemen	Vanuit R-schijf worden databestanden verzonden via RIVM Filesender
	Andere processen	RIVM filesender wordt breed gebruikt binnen het RIVM.
	Kritische momenten	De momenten waarop RIVM de databestanden deelt met de externe gebruikers.
	Soort informatie	<i>Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?)</i> Privacygevoelige informatie. Zie ook de toelichting bij Survalyzer Nederland BV.
	Data rubricering¹	<i>Welke classificatie is van toepassing op de informatie? (Openbaar, RIVM intern, RIVM vertrouwelijk, Departementaal Vertrouwelijk, Stg. Confidentieel, Stg. Geheim, Stg. Zeer Geheim)</i> RIVM vertrouwelijk
	Externe eisen	<i>Denk hierbij aan eisen vanuit de AVG, NAVO, EU, ketenpartner(s) en evt. andere organisatie(s).</i> AVG is van toepassing i.v.m. privacygevoelige informatie.

C4	RIVM StatLine	
	Eigenaar informatiesysteem	IV-organisatie
	De gebruikers van het informatiesysteem	<i>Degene die werkzaam zijn met het informatiesysteem</i> - Interne gebruiker / klant: RIVM - Externe gebruiker / klant: onderzoekers, beleidsmakers - Aantal gebruikers: enkele aangewezen personen binnen het RIVM.
	De output van het informatiesysteem	Publicatie op RIVM statline / VZ info
	Koppelvlakken met andere informatiesystemen	Vanuit R-schijf wordt tabel ingelezen op RIVM StatLine
	Andere processen	StatLine wordt breed gebruikt binnen het RIVM.
	Kritische momenten	<i>Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes.</i> Publicatiemoment op dinsdag 28 mei 2024, belangrijk dat RIVM StatLine dan bezocht kan worden.
	Soort informatie	<i>Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?)</i> Privacygevoelige informatie. Zie ook de toelichting bij Survalyzer Nederland BV.
	Data rubricering¹	<i>Welke classificatie is van toepassing op de informatie? (Openbaar, RIVM intern, RIVM vertrouwelijk, Departementaal Vertrouwelijk, Stg. Confidentieel, Stg. Geheim, Stg. Zeer Geheim)</i> RIVM vertrouwelijk
	Externe eisen	<i>Denk hierbij aan eisen vanuit de AVG, NAVO, EU, ketenpartner(s) en evt. andere organisatie(s).</i> N.v.t., geaggregeerde gegevens

C5	Digital Research Environment	
	Eigenaar informatiesysteem	IV-organisatie
	De gebruikers van het informatiesysteem	<i>Degene die werkzaam zijn met het informatiesysteem</i> - Interne gebruiker / klant: RIVM - Externe gebruiker / klant: onderzoekers - Aantal gebruikers: enkele aangewezen personen binnen het RIVM, onderzoekers die een

		data-aanvraag hebben gedaan welke is goedgekeurd door de registratiecommissie van de Gezondheidsmonitors.
	De output van het informatiesysteem	Onderzoeksresultaten van derden.
	Koppelvlakken met andere informatiesystemen	Vanuit R-schijf wordt databestand geupload naar Digital Research Environment
	Andere processen	De Digital Research Environment wordt steeds meer gebruikt binnen het RIVM.
	Kritische momenten	<i>Beschrijf de kritische momenten dat het informatiesysteem gebruikt wordt. Bijvoorbeeld de piekperiodes.</i> Als er meerdere aanvragen tegelijkertijd binnenkomen.
	Soort informatie	<i>Beschrijf wat voor soort informatie in het informatiesysteem wordt verwerkt (is dit privacygevoelige informatie, commercieel vertrouwelijke informatie, politiek gevoelige informatie?)</i> Privacygevoelige informatie. Zie ook de toelichting bij Survalyzer Nederland BV.
	Data rubricering¹	<i>Welke classificatie is van toepassing op de informatie? (Openbaar, RIVM intern, RIVM vertrouwelijk, Departementaal Vertrouwelijk, Stg. Confidentieel, Stg. Geheim, Stg. Zeer Geheim)</i> RIVM vertrouwelijk
	Externe eisen	<i>Denk hierbij aan eisen vanuit de AVG, NAVO, EU, ketenpartner(s) en evt. andere organisatie(s).</i> AVG is van toepassing i.v.m. privacygevoelige 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 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
Online vragenlijst Gezondheidsmonitor Jeugd 2023	B	Het proces 'Online vragenlijst Gezondheidsmonitor Jeugd 2023' is als bijdragend geclassificeerd. Het betreft zeker geen hoofdactiviteit van het centrum VPZ, maar is wel bijdragend aan haar primaire processen. Het valt onder het deelproces "Dataverzameling (kwantitatief en kwalitatief) t.b.v onderzoek en evaluatie op het gebied van gezondheid, preventie en zorg", net als verschillende andere gezondheidsmonitors van het centrum.

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
Survalyzer Nederland BV		N
Survalyzer Nederland BV wordt als nuttig geclassificeerd voor het proces van de Online vragenlijst Gezondheidsmonitor Jeugd 2023. De vragenlijsten moeten wel online kunnen worden uitgezet, want schriftelijk uitzetten zou onevenredig veel extra inspanning vragen, maar hierbij is Survalyzer als online tool niet per se essentieel. Er zijn vele andere alternatieven beschikbaar.		

<i>Smartlockr</i>	N	Er zijn verschillende alternatieven denkbaar, dus dit platform is geclassificeerd als nuttig.
<i>Filesender</i>	N	Er zijn verschillende alternatieven denkbaar, dus dit platform is geclassificeerd als nuttig.
<i>RIVM statline</i>	B	Er is geen alternatief voor RIVM StatLine, dus dit platform is geclassificeerd als belangrijk.
<i>Digital Research Environment</i>	N	Er zijn verschillende alternatieven denkbaar, dus dit platform is geclassificeerd als nuttig.

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
Survalyzer Nederland BV		N.v.t.	-	Niet van het RIVM. Zijn geen eisen aan verbonden. Laag zou anders passend zijn.
Smartlockr		N.v.t.	-	Niet van het RIVM. Zijn geen eisen aan verbonden. Laag zou anders passend zijn.
Filesender RIVM		Laag	Er is 1 moment in het jaar, waarbij je wilt dat Filesender binnen 24 uur weer beschikbaar is. En dat is bij de deadline dat de GGD wacht op data van het RIVM	Mocht Filesender niet beschikbaar zijn, kan de GGD niet tijdig data ontvangen, dit valt onder interne negatieve publiciteit.
RIVM Statline		Laag		Vervelend indien niet beschikbaar, maar heeft een lage impact.
DRE		Laag		Vervelend indien niet beschikbaar, maar heeft een lage impact.

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	
Survalyzer Nederland BV		Laag	De impact voor integriteit wordt geclassificeerd op 'laag'. Indien juistheid en/of volledigheid van gegevens in het systeem niet op orde zijn kan dit beperkte tot wat grotere schade opleveren voor het RIVM, afhankelijk van de fout. Resultaten van de monitor kunnen een vertekend / verkeerd beeld geven aan de buitenwereld, bijvoorbeeld bij dataverlies, met alle gevolgen van dien. Mensen kunnen de cijfers bijvoorbeeld niet meer serieus nemen of het project kan worden vertraagd. Dit alles kan resulteren in ongemak of serieuze klachten onder de maatschappij, maar niet tot de gevolgen die bij Midden en Hoog staan beschreven.	

<i>Smartlockr</i>	<i>Laag</i>	Zelfde motivatie als voor Survalyzer. De data die met Survalyzer is verzameld wordt via Smartlockr beschikbaar gesteld aan het RIVM en de GGD'en. Spelen hier problemen rond de juistheid en/of volledigheid van de gegevens dan kan dit leiden tot dezelfde gevolgen.
<i>Filesender</i>	<i>Laag</i>	De impact voor integriteit wordt geclassificeerd op 'laag'. Indien juistheid en/of volledigheid van gegevens in het systeem niet op orde zijn kan dit beperkte tot wat grotere schade opleveren voor het RIVM, afhankelijk van de fout. Resultaten van de monitor kunnen een vertekend / verkeerd beeld geven aan de buitenwereld, bijvoorbeeld bij dataverlies, met alle gevolgen van dien. Mensen kunnen de cijfers bijvoorbeeld niet meer serieus nemen of het project kan worden vertraagd. Dit alles kan resulteren in ongemak of serieuze klachten onder de maatschappij, maar niet tot de gevolgen die bij Midden en Hoog staan beschreven.
<i>RIVM Statline</i>	<i>Laag</i>	De impact voor integriteit wordt geclassificeerd op 'laag'. Indien juistheid en/of volledigheid van gegevens in het systeem niet op orde zijn kan dit beperkte tot wat grotere schade opleveren voor het RIVM, afhankelijk van de fout. Resultaten van de monitor kunnen een vertekend / verkeerd beeld geven aan de buitenwereld, bijvoorbeeld bij dataverlies, met alle gevolgen van dien. Mensen kunnen de cijfers bijvoorbeeld niet meer serieus nemen of het project kan worden vertraagd. Dit alles kan resulteren in ongemak of serieuze klachten onder de maatschappij, maar niet tot de gevolgen die bij Midden en Hoog staan beschreven.
<i>DRE</i>	<i>Laag</i>	De impact voor integriteit wordt geclassificeerd op 'laag'. Indien juistheid en/of volledigheid van gegevens in het systeem niet op orde zijn kan dit beperkte tot wat grotere schade opleveren voor het RIVM, afhankelijk van de fout. Resultaten van de monitor kunnen een vertekend / verkeerd beeld geven aan de buitenwereld, bijvoorbeeld bij dataverlies, met alle gevolgen van dien. Mensen kunnen de cijfers bijvoorbeeld niet meer serieus nemen of het project kan worden vertraagd. Dit alles kan resulteren in ongemak of serieuze klachten onder de maatschappij, maar niet tot de gevolgen die bij Midden en Hoog staan beschreven.

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>	- 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 <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	
<i>Survalyzer Nederland BV</i>		<i>Midden</i>	Indien de vertrouwelijkheid van dit systeem wordt geschaad kan dit tot forse consequenties hebben. In het systeem staat privacygevoelige informatie van scholieren. Imagoschade voor het RIVM als partner behoort tot de risico's bij een datalek. Het kan onrust geven in het publieke domein en voor reputatieschade zorgen voor de Gezondheidsmonitor. Misschien willen mensen dan niet meer meedoen in het vervolg.	
<i>Smartlockr</i>		<i>Midden</i>	Zelfde motivatie als Survalyzer.	
<i>RIVM Filesender</i>		<i>Midden</i>	Zelfde motivatie als Survalyzer.	
<i>RIVM statline</i>		<i>Laag</i>	Betreft openbare geaggregeerde data	

Digital Research Environment	Midden	Zelfde motivatie als Survalyzer.
------------------------------	--------	----------------------------------

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	X	Nuttig	X	Laag	X	Laag		Laag
		RIVM Intern (besloten)	X	Bijdragend		Belangrijk		Midden		Midden	X	Midden
	X	RIVM Vertrouwelijk		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	Er kan imagoschade optreden voor de organisatie indien er een breuk in vertrouwelijkheid of betrouwbaarheid is, dus er wordt gekozen voor BBN2. Er is privacygevoelige informatie van scholieren (deelnemers aan de vragenlijsten) bij betrokken in verschillende gebruikte systemen in dit proces en gelet op de onderwerpen van de vragen kun je sommige informatie ook als medische informatie beschouwen. De vragenlijsten bevatten een aantal gevoelige onderwerpen die iets zeggen over iemands gezondheid. BBN2 is niet te zwaar (een adequate beveiliging is nodig i.v.m. de vertrouwelijkheid van de gegevens) en ook niet te licht (er zijn geen sterke dreigingen of hoge eisen).
	RTO 5dgn, 2dgn of < 2dgn	N.v.t.	De ondersteunende systemen zijn niet van het RIVM. Dergelijke eisen zijn hier niet aan verbonden geweest.
	RPO 28hr, 24hr of <24hr	N.v.t.	De ondersteunende systemen zijn niet van het RIVM. Dergelijke eisen zijn hier niet aan verbonden geweest.
	Externe eisen NAVO, EU, ketenpartner, andere organisatie, AVG	Ja	AVG is van toepassing i.v.m. privacygevoelige informatie.
	Uitvoeren Risicoanalyse? Ja of nee	Nee	De systemen Survalyzer en Smartlockr zijn niet van het RIVM. De overeenkomst voor deze monitor is gesloten tussen het RIVM, de GGD'en en Research 2Evolve. RIVM is een van de verwerkingsverantwoordelijken en heeft dus een bepaalde medeverantwoordelijkheid op het gebied van informatiebeveiliging in het geheel.

Tekenformulier		
Op 21 augustus 2023 heeft een workshop QuickScan Information Security plaatsgevonden voor Online vragenlijst Gezondheidsmonitor Jeugd 2023 met ondersteunende informatiesystemen Survalyzer Nederland BV, Smartlocker, RIVM filesender, RIVM Statline en Digital Research Environment.		
Bij deze workshop waren aanwezig:		
Naam	Functie	Afdeling

5.1.2.e
5.1.2.e
5.1.2.e

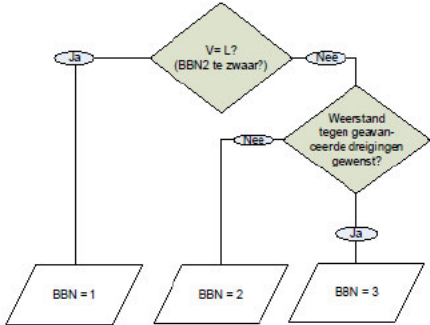
5.1.2.e
5.1.2.e
5.1.2.e

5.1.2.e
5.1.2.e
5.1.2.e

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 tijd vereisen? 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 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: - 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? - Worden er wettelijke eisen aan de vertrouwelijkheid gesteld (bijv. AVG)? - Zijn er contractuele verplichtingen qua vertrouwelijkheid afgesproken naar burgers? - Zijn er resultaten van andere Quickscans die leiden tot hogere vertrouwelijkheidseisen? - 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: - het BBN-niveau. BBN3 niveau is van toepassing indien dreiging heerst vanuit statelijke actoren. - RPO en RTO eisen - 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.  Toelichting: Geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), gaan uit van een doelgerichte 'langdurige' cyberaanval op vooral kennisrijke landen en organisaties door statelijke actoren en criminele organisaties. De aanval is daarbij volhardend in zowel de pogingen om een organisatie binnen te dringen als ook om binnen de ICT-infrastructuur heimelijk aanwezig te blijven.