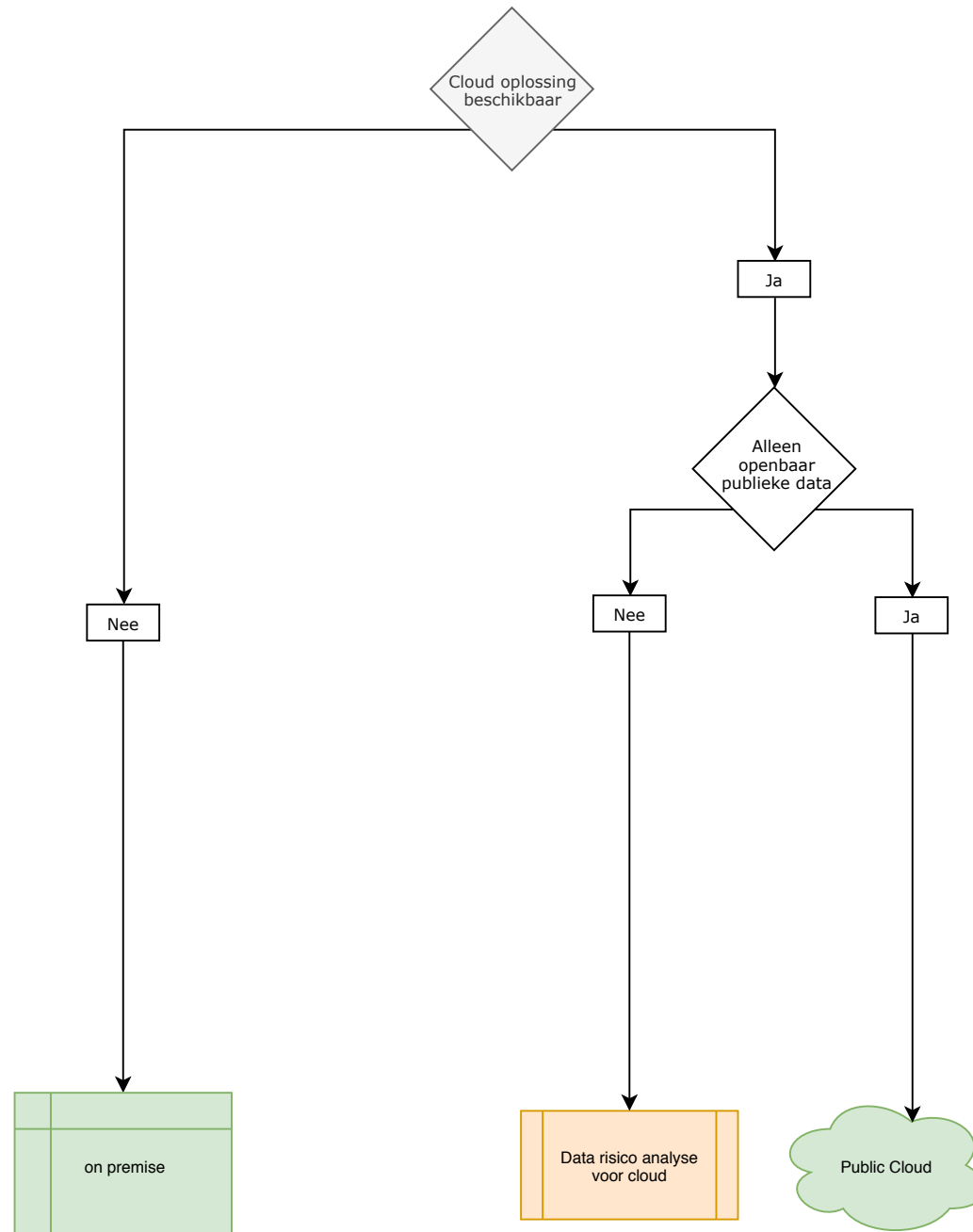


Cloud readiness analyse

Bepaal of de leverancier een "SAAS"oplossing kan aanbieden.



Beschikbaarheids Analyse voor cloud

Beschikbaarheid stelt in tegenstelling tot integriteit en vertrouwelijkheid geen eisen aan de inhoud van de data. Er gelden daarom geen bijzondere maatregelen voor authenticatie, autorisatie, monitoring en beveiliging, zoals voor integriteit en vertrouwelijkheid (zie volgende paragrafen). Aangezien de normen voor beschikbaarheid verschillen per service moet het classificatieniveau voor beschikbaarheid altijd worden gespecificeerd.

Beschikbaarheid is gedefinieerd als 'eigenschappen van het geheel van ICT-diensten, systemen, componenten en gegevensdragers die van invloed zijn op de tijd dat het product of de dienst (en daarmee informatie) beschikbaar is voor de geautoriseerde gebruiker, op de momenten dat het beschikbaar moet zijn'. Beschikbaarheid wordt gemeten aan de hand van de Mean Time Between Failures (MTBF). Dit is de gemiddelde tijd tussen het herstel van het ene incident en het optreden van het volgende incident.

Gevolgen van het niet beschikbaar hebben van de benodigde informatie of gegevens. (in het ergste geval)		Waardering (uur, dag, week, maand)				Argumentatie (verplicht invullen)
		1u	1d	1w	1m	
B1	Besluitvorming: Na welke tijdsduur is het ontbreken van informatie nadelig voor het nemen van management beslissingen?	0	0	1	2	De waardering moet ingevuld worden voor alle tijdseenheden en met een waarde van 0 tot en met 3, zie waarderingsschaal onderaan
B2	Imagoverlies Hoe lang duurt het voordat er sprake is van imagoverlies wanneer informatie niet voorhanden is?	0	1	2	2	
B3	Hapering dienstverlening Hoe lang kan het systeem c.q. de informatie niet beschikbaar zijn voordat er haperingen in het proces optreden welke de dienstverlening aan burgers/bedrijven/ketenpartners raakt?	1	1	2	2	<Dataverlies (Recovery-Point Objective (RPO)) en hersteltijd (Recovery-Time Objective (RTO)) zijn doelstellingen die een belangrijke rol spelen bij disaster recovery. Hoeveel dataverlies (RPO) is acceptabel en binnen welke tijdsperiode (RTO) moet de dienstverlening weer hersteld zijn? Deze vraag heeft betrekking op de hersteltijd (RTO). Vraag B7 heeft betrekking op het dataverlies (RPO).>
B4	Wettelijke aansprakelijkheid: Hoe lang kan de applicatie of informatie niet beschikbaar zijn voordat er wettelijke of contractuele verplichtingen niet kunnen worden nagekomen?	0	0	1	1	
B5	Additionele kosten: Na welke periode zijn additionele kosten voor de organisatie te verwachten, bij het niet beschikbaar zijn van de applicatie of informatie?	0	0	0	1	
B6	Moreel van de medewerkers: Na welke periode is er sprake van een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers, wanneer de informatievoorziening hapert?	0	0	1	2	
B7	Herstel: Hoe lang mag het herstellen na een onbeschikbaarheid van informatie duren voordat er daadwerkelijk hapering in de dienstverlening aan burgers/bedrijven/ketenpartners ontstaat? Zijn er hoge herstelkosten? Dus achteraf verwerken van verloren gegaan werk. Denk ook aan: het herstellen van verloren gegaan werk	0	0	2	2	<Dataverlies (Recovery-Point Objective (RPO)) en hersteltijd (Recovery-Time Objective (RTO)) zijn doelstellingen die een belangrijke rol spelen bij disaster recovery. Hoeveel dataverlies (RPO) is acceptabel en binnen welke tijdsperiode (RTO) moet de dienstverlening weer hersteld zijn? Deze vraag heeft betrekking op het dataverlies (RPO).> Vraag B3 heeft betrekking op de hersteltijd (RTO).
Wat is de meest serieuze impact als het proces onbeschikbaar is?		1	1	2	2	<Neem de hoogste score, per kolom, over van bovenstaande ingevulde impact waarderingen.>
Wat is overall de meest serieuze impact als het proces onbeschikbaar is?		2				<Neem de totale score over van bovenstaande ingevulde impact typering.>

Invulinstructie

Bij beschikbaarheid is het van belang om bij verschillende uitvalstermijnen de schade te weten. Daarom dient per regel, dus per beschikbaarheidsvraag, in iedere kolom een schade waarderingscijfer (bijvoorbeeld 0, 1, 2 of 3) te worden aangegeven.

Tevens dient hierbij een onderbouwing te worden gegeven waarom gekozen is voor de betreffende waarderingscijfers.

De impact op het bedrijfsproces wordt beoordeeld op basis

0. Verwaarloosbare schade
1. Belangrijke schade
2. Ernstige schade
3. Bedreigt het voortbestaan van de gemeente

Eindoordeel

Niet nodig 0
De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.

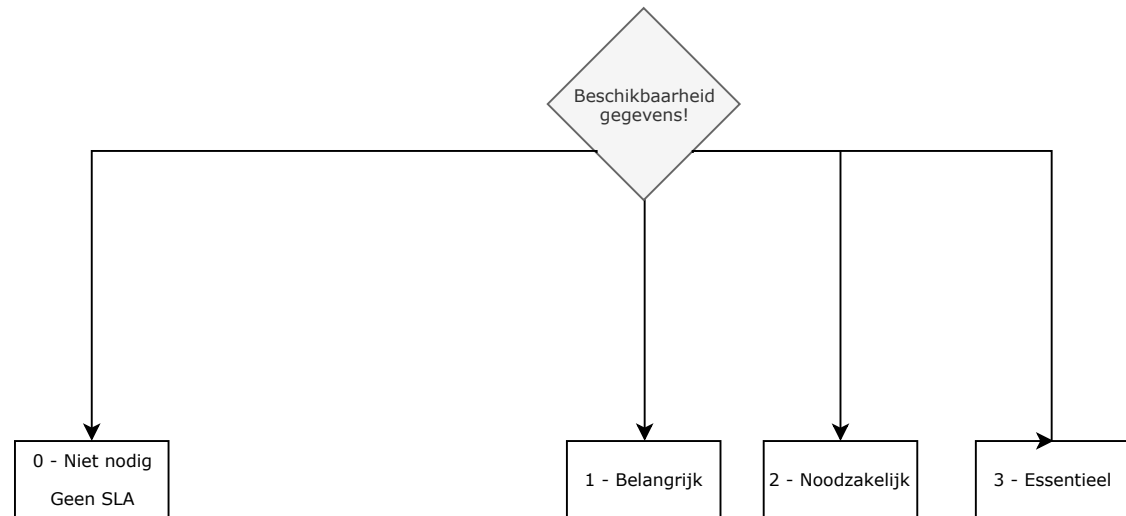
Belangrijk 1
De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen.

Noodzakelijk 2
De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schadetoebrengen.

Essentieel 3
De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van beschikbaarheid kan (zeer) grote schade toebrengen.

Beschikbaarheids Analyse voor cloud

Aan de hand van uitkomst van de vragenlijst beschikbaarheid, moet de "cloud" oplossing voldoen aan de onderstaande beschikbaarheidseisen.



Beschikbaarheid			
Werktijden	08:00 - 17:00 maandag t/n vrijdag behoudens algemeen erkende feestdagen	08:00 - 21:00 maandag t/n vrijdag behoudens algemeen erkende feestdagen	24 * 7 behoudens gepland onderhoud
Beschikbaarheid tijdens werktijd	min 99,6%	min 99,6%	min 99,9%
Beschikbaarheid buiten werktijd	min 96,1%	min 96,1%	N.V.T.
Mean Time Between Failures (MTBF)	min 100 dagen	min 100 dagen	min 200 dagen
Mean Time To Repair (MTTR)	max 4 uur	max 4 uur	max 4 uur
Maximaal aantal storingen van 3 minuten of korter	4x per maand	2x per maand	1x per maand
Maximaal aantal storingen van langer dan drie minuten	1x per maand	1x per 2 maanden	1x per half jaar

Eindoordeel

Niet nodig 0
De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.

Belangrijk 1
De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen.

Noodzakelijk 2
De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schadetoebrengen.

Essentieel 3
De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van beschikbaarheid kan (zeer) grote schade toebrengen.

Vragenlijst integriteit

Het onderwerp integriteit valt normaliter in twee delen uiteen: de integriteit van datacommunicatie en opslag enerzijds (d.w.z. niet gerelateerd aan het gemeentelijke proces zelf), en de integriteit van de informatie in de applicaties of fysiek (d.w.z. gerelateerd aan het gemeentelijke proces zelf). Integriteit gekoppeld aan de applicatie is altijd situatie afhankelijk en afhankelijk van de eisen van een specifiek proces. Voor de functionele integriteit van de informatievoorziening wordt een minimale set van normen opgesteld waarbij er per dienst en/of applicatie nadere afspraken gemaakt kunnen worden.

Integriteit geeft de mate aan waarin de informatie actueel en correct is. Kenmerken zijn juistheid, volledigheid en tijdigheid van de transacties.

Gevolgen van fouten in informatie of doelbewuste manipulatie van informatie om te frauderen of fraude te maskeren (in het eerste geval)		Waardering				Argumentatie (verplicht invullen)
I1	Managementbeslissingen: Hoe schadelijk is het als op basis van deze informatie verkeerde managementbeslissingen worden genomen?	3	2	1	0	<Kies 1 (één) van de waardes per rij!>
I2	Fraude potentie: Welke impact hebben frauduleuze handelingen?	3	2	1	0	
I3	Onderbreking van het proces: In hoeverre wordt het proces onderbroken als gevolg van ongeautoriseerde wijzigingen van, of fouten in de informatie?	3	2	1	0	
I4	Vertrouwen van het publiek c.q. klanten: Kan het vertrouwen van het publiek geschaad worden door onjuiste informatie welke in het proces wordt verwerkt?	3	2	1	0	
I5	Wettelijke aansprakelijkheid: Wat kunnen de gevolgen zijn van het niet voldoen aan wettelijke of contractuele verplichtingen die veroorzaakt worden door onjuiste informatie welke in het proces wordt verwerkt?	3	2	1	0	
I6	Additionele kosten: In hoeverre kunnen er additionele kosten ontstaan door het verwerken van onjuiste informatie in het proces? Bijvoorbeeld door het moeten herstellen van een corrupte database of opnieuw invoeren van gegevens..	3	2	1	0	
I7	Moreel van de medewerkers: Wat zijn de schadelijke effecten op het moreel van medewerkers als er onjuiste informatie verwerkt in het proces	3	2	1	0	
	Totaalscore In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door fouten of ongeautoriseerde wijzigingen? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)		2			
3 =	Absoluut: zeer ernstige schade: raadvragen, kamervragen, reactie minister of wethouder vereist, belangrijke partners/klanten stellen professionaliteit van het rijk of de gemeentelijke dienst ter discussie.					
2 =	Hoog: ernstige schade: krantenkoppen, vragen van belangrijke partners/klanten, burgers budgettaire problemen					
1 =	Beschermd: acceptabele schade, binnen marges: incident met direct betrokkenen is snel recht te zetten.					
0 =	Niet Zeker: Verwaarloosbare schade of niet van toepassing.					

Invulinstructie

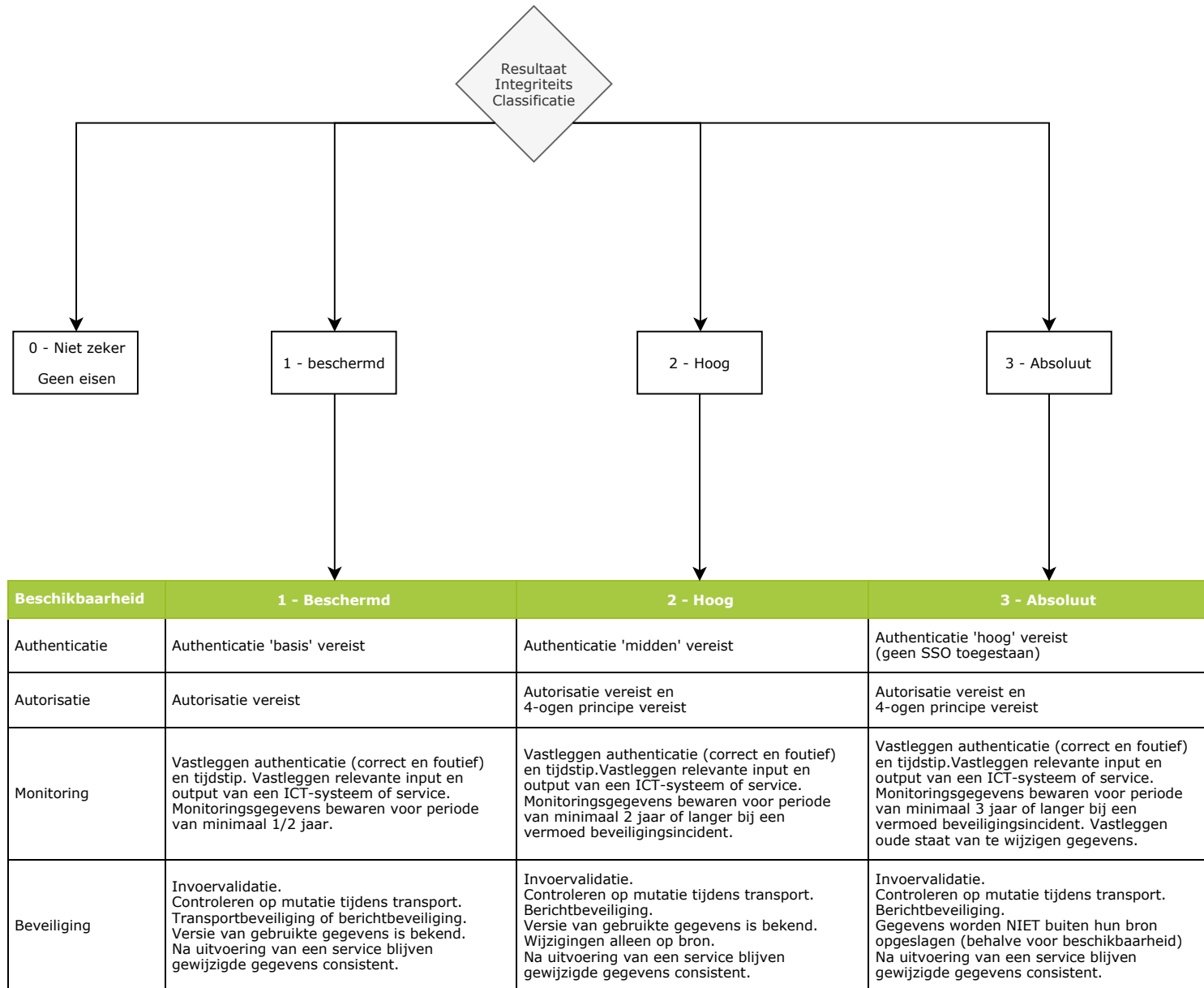
De impact op het bedrijfsproces wordt beoordeeld op basis

- 0. Verwaarloosbare schade
- 1. Acceptabele schade
- 2. Ernstige schade
- 3. Zeer ernstige schade

Tevens dient hierbij een onderbouwing te worden gegeven waarom gekozen is voor de betreffende waarderingcijfers.

Integriteitsanalyse voor cloud

Aan de hand van uitkomst van de vragenlijst integriteit, moet de "cloud" oplossing voldoen aan de onderstaande beveiligingseisen.



Vragenlijst vertrouwelijkheid

Vertrouwelijkheid is het kwaliteitsbegrip waaronder privacybescherming maar ook de exclusiviteit van informatie gevangen kan worden. Het waarborgt dat alleen geautoriseerden toegang krijgen en dat informatie niet kan uitlekken.

Vertrouwelijke gegevens zijn bijvoorbeeld:

- Persoonsgegevens
- Gemeentelijke- en bedrijfsgeheimen
- Concurrentiegevoelige gegevens zoals voorbereidingen voor bestemmingsplannen
- Medische gegevens

Bedrijfsproces consequentie (in het ergste geval)		Waardering				Argumentatie (verplicht invullen)
V1	Vertrouwen van de burger: Wat zijn de gevolgen voor de gemeente indien de binnen het proces beschikbare informatie te vroeg c.q. niet volgens de regels verspreid wordt?	3	2	1	0	<Kies 1 (één) van de waardes per rij!>
V2	Publiek vertrouwen: Hoe groot is de imago schade als deze informatie publiek wordt, hoe groot zijn de nadelige gevolgen voor het vertrouwen dat onze burgers (onze omgeving) in ons hebben?	3	2	1	0	
V3	ketensamenwerking: Kan de gemeente toegang tot de keten in het proces geweigerd worden?	3	2	1	0	
V4	Vertrouwen van ketenpartners : Wat zijn de gevolgen voor de relatie met de ketenpartners, als vertrouwelijke informatie onterecht wordt verspreid.?	3	2	1	0	
V5	Aansprakelijkheid: Wat zijn de gevolgen voor (wettelijke) aansprakelijkheid bij het onterecht verspreiden van deze informatie?	3	2	1	0	
V6	Additionele kosten: In hoeverre is er sprake van additionele kosten door onterechte verspreiding van deze informatie?	3	2	1	0	
V7	Moreel van de medewerkers: In hoeverre kan een duidelijk negatieve invloed op het moreel en de motivatie van medewerkers een gevolg zijn van de onterechte verspreiding van deze informatie?	3	2	1	0	
Totaalscore In samenvatting: gegeven de bovenstaande scores (en eventueel andere consequenties) wat is dan de grootste schade die kan ontstaan door het onbedoeld openbaar maken of verliezen van informatie of ongeautoriseerde toegang bieden tot deze informatie? (dit zou normaal minimaal gelijk moeten zijn aan de grootste schade op individuele basis)		3				
3	zeer ernstige schade: raadvragen, reactie wethouder vereist, belangrijke partners /klanten stellen professionaliteit van de gemeentelijke dienst ter discussie.					
=						
2 =	ernstige schade: krantenkoppen, vragen van belangrijke partners /politiek/burgers afnemers.					
1 =	acceptabele schade, binnen marges: incident met direct betrokkenen is snel recht te zetten.					
0 =	verwaarloosbare schade of niet van toepassing.					

Invulinstructie

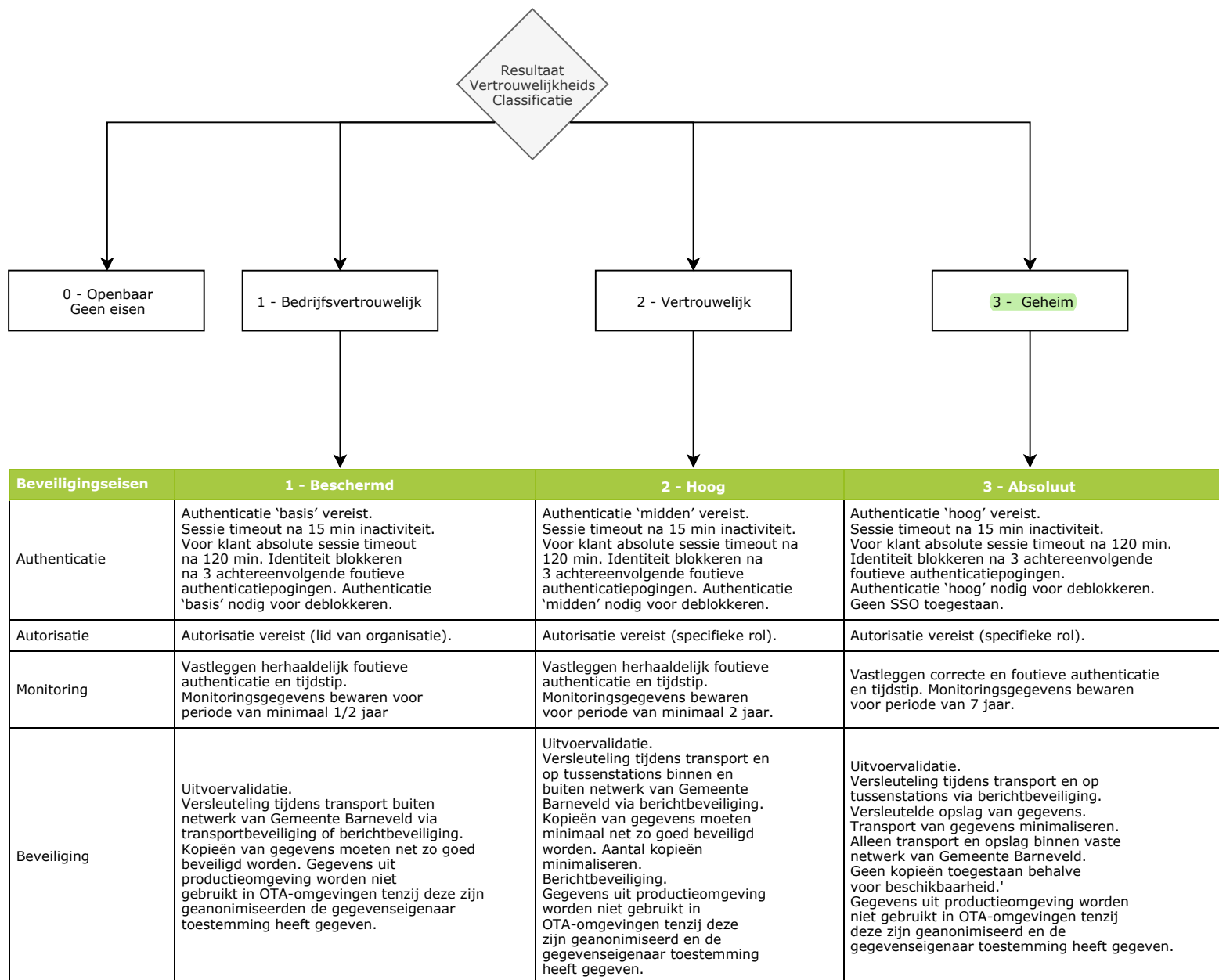
De impact op het bedrijfsproces wordt beoordeeld op basis

0. Verwaarloosbare schade
1. Acceptabele schade
2. Ernstige schade
3. Zeer ernstige schade

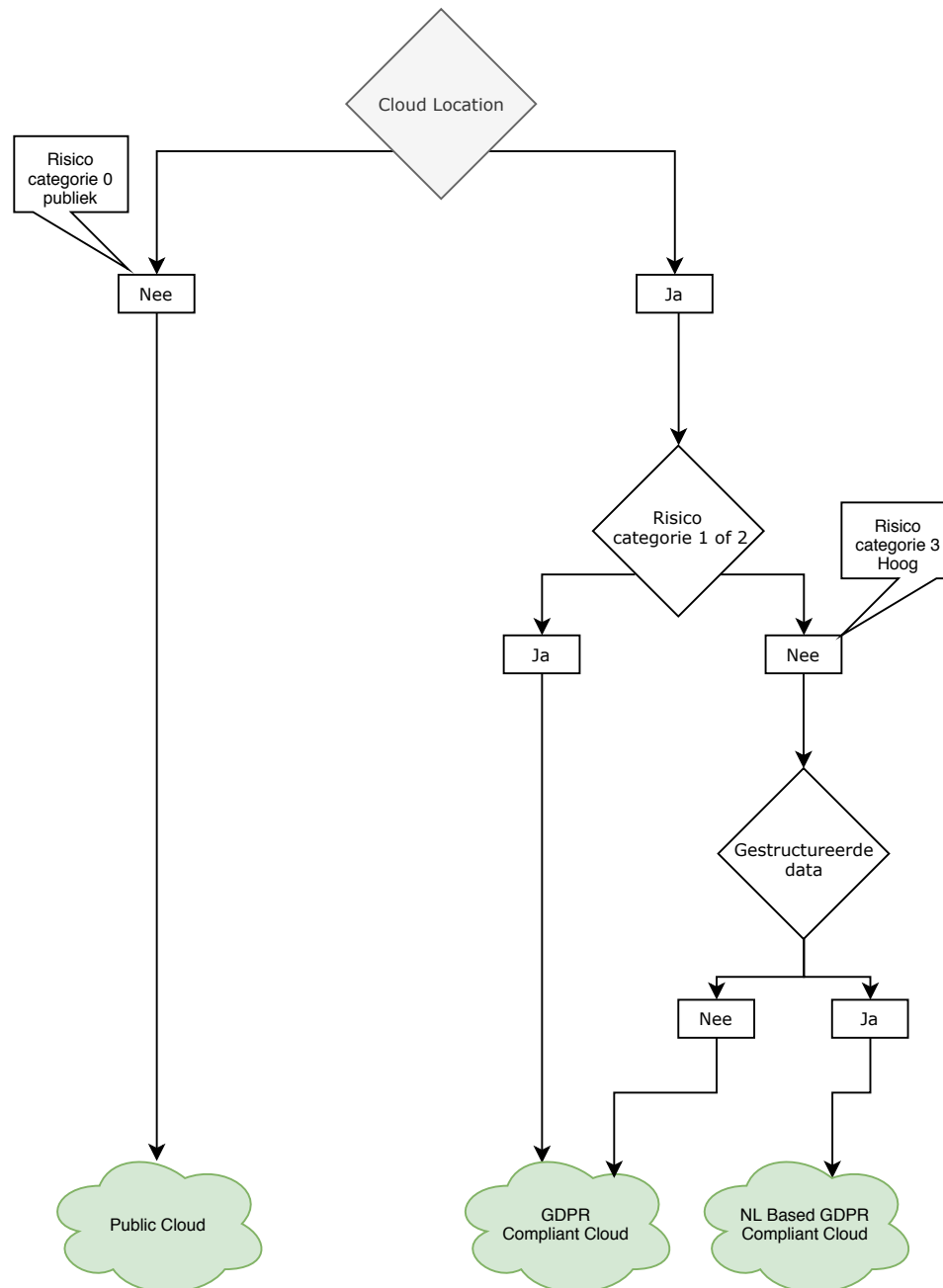
Tevens dient hierbij een onderbouwing te worden gegeven waarom gekozen is voor de betreffende waarderingscijfers.

Vertrouwelijkheidsanalyse voor cloud

Aan de hand van uitkomst van de vragenlijst Vertrouwelijkheid, moet de "cloud" oplossing voldoen aan de onderstaande beveiligingseisen.



Afhankelijk van het bepaalde risico categorie zal worden aangegeven wat de geografisch locatie van de cloud zal zijn.



Risicocategorie 0 (Openbaar/publiek niveau.)

Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.

Eis(en): Geen eisen vanuit cloudbeleid

Risicocategorie 1 (Bedrijfsvertrouwelijk)

Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.

Eis(en): Cloudprovider moet GDPR compliant zijn.

Risicocategorie 2 (verhoogd niveau/vertrouwelijk)

Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.

Eis(en): Cloudprovider moet GDPR compliant zijn.

Risicocategorie 3 (Hoog risico/geheim)

Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen

Eis(en): Cloudprovider moet GDPR compliant zijn.

Gestructureerde data mag alleen binnen Nederland worden gehost. (databases, spreadsheets, applicatiedata etc.)