Non-functional user stories ten behoeve van informatiebeveiliging voor Common Ground

Deze sheets bevatten de resultaten van een risicoanalyse voor Common Ground die is uitgevoerd om te komen tot non-functional user stories ten behoeve van informatiebeveiliging voor diverse stakeholders.

Doel:
De user stories kunnen worden gebruikt door ontwikkelteams (bij gemeenten of toeleveranciers) die oplossingen ontwikkelen in het kader van Common Ground. Zij kunnen de stories as-is gebruiken, of als leidraad dienen bij het opstellen van definitions of done. Bovendien kunnen de user stories bij inkoop van (software)producten of softwareontwikkeling door derden gebruikt worden als basis voor eisen ten aanzien van informatiebeveiliging.

De volgende kolommen zijn van belang:

1. Soort incident en Scope RA	Is het incident interessant voor deze Risico Analyse?
2. Schade en Kans	Hoe hoog worden kans en schade ingeschat, de impact
3. Scope maatregel	Leiden schade en kans tot een niveau van risico zodat er een user story nodig is
4. Toelichting/gevolgen etc.	Omschrijving duiding risico
5. Ontwikkelaar/architect userstory	Welke user stories zijn er voor ontwikkelaars en architecten om dit risico te
6. User userstory	Welke user stories zijn er dan voor eindgebruikers om dit risico te verlagen?
7. CG organisatie userstory	Welke user stories zijn er dan voor de CG organisatie als geheel (of toeleveranciers) om dit risico te verlagen?

Bij het opstellen van deze stories is niet gekeken naar detailvragen van mogelijke oplossingen, bijvoorbeeld softwareproducten. Als er aan een detail oplossing gewerkt gaat worden dan moet er opnieuw op basis van risico gekeken worden naar aanvullende userstories (privacy, Cloud voorzieningen, Web toepassingen en apps.

De user stories:
De user stories zijn beschreven vanuit 3 perspectieven: de ontwikkelaar/architect, de user van het product en Common Ground/leverancier.
1: De ontwikkelaar/architect userstories gelden in principe voor alle ontwikkelaars van CG producten of diensten, onafhankelijk van waar of voor wie zij werken.
2: De gebruiker (user) stories zijn beschreven vanuit de optiek van de eindgebruiker bij de gemeente, de klant.
3: De Common Ground Userstories zijn beschreven vanuit de optiek van de aansturende organisatie, dit kan Common Ground als grote aansturende organisatie, maar ook een leverancier.

Dit is een levend document, er kunnen altijd meer details of aandachtspunten ontstaan de leiden tot meer of minder of aangepaste userstories.

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
Mens	**Wegvallen:**	n					Wegvallen mens is out of scope			
· Functioneert onjuist	· Voorzienbaar (ontslag, vakantie)	n								
· Niet aanwezig	· Onvoorzienbaar (ziekten, overlijden, ongeval, staking)	n								
· Niet in dienst		n								
		n								
	Onopzettelijk foutief handelen:	j								
mens	· Onkunde, slordigheid	j	M	L	M L	j	Deze kans is er altijd ingeschat als medium, nieuwe software moet dit ondervangen en daarnaast moet er aandacht zijn voor opleiden	Zie documentatie eisen Als ontwikkelaar realiseer ik software die fouten zoals onkunde en slordigheid afvangt en daarnaast heldere scherm boodschappen geeft aan de eindgebruiker bij mogelijke fouten of gewoon om de eindgebruiker te ondersteunen.	Als eindgebruiker wil ik dat mijn fouten bij gebruik van CG software producten worden ondervangen door de software zodat ik in staat ben foutloos te werken. Als eindgebruiker wil ik duidelijke status en foutmeldingen bij gebruik van de software zodat ik in staat ben zonder fouten te werken en foutsituaties op kan lossen	Als common ground dragen we zorg voor architecten, ontwikkelaars, testers die goed zijn opgeleid om de kans op fouten zo klein mogelijk te maken. Met goed wordt hier bedoeld de relevante opleidingen en ervaring voor het werk dat gedaan moet worden.
mens	· Foutieve procedures	j	M	L	M L	j	Deze kans is er altijd ingeschat als medium, nieuwe software moet dit ondervangen en daarnaast moet er aandacht zijn voor opleiden. Het gaat hier ook om foutieve eindgebruikers procedures in relatie tot gebruik van de software	Als ontwikkelaar werk ik volgens vastgestelde procedures en common ground afspraken om de kans op fouten te verminderen. Als ontwikkelaar maak ik voor al mijn producten voldoende documentatie zodat eindgebruikers goede handleidingen hebben voor het gebruik van het product in hun situatie.	Als eindgebruiker wil ik dat ik geholpen wordt met het juist gebruiken van de software door middel van aanwijzingen en documentatie en opleidingen zodat ik behoed wordt tegen het maken van fouten.	Als common ground zorgen we voor voldoende procedures en stellen deze bekend om er voor te zorgen dat de schade van fouten zo laag mogelijk te houden. Procedures zijn: ontwikkelaanpak, professionele ondersteuning, testen en testaanpak, software kwaliteitsstandaarden, gestandaardiseerde ontwikkelomgevingen
mens	· Complexe foutgevoelige bediening	j	M	M	M M	j	systemen moeten makkelijk te begrijpen en te bedienen zijn	Als ontwikkelaar maak ik software die gebruikt kan worden door de doelgroep waarvoor ik het maak en past bij de doelgroep waarvoor ik het maak, de software die ik maak is eenvoudig te bedienen. Software moet eenvoudig te gebruiken zijn en de kans op fouten verminderen. Nog nadenken wat dit soms voor burgers kan betekenen	Als eindgebruiker wil ik dat de software die ik ga gebruiken eenvoudig gebruikt kan worden en dat ik goede aanwijzingen krijg om de kans op fouten te verminderen. Als eindgebruiker van het product of dienst wil ik een gebruikershandleiding kunnen raadplegen zodat ik geholpen wordt bij het gebruikt van dat product of dienst.	
mens	· Onzorgvuldige omgang met wachtwoorden	j	H	L	H L	j	Dit is niet direct een risico van CG als het om de eindgebruiker gaat, maar wel reëel, geldt met name voor gemeenten.	Als ontwikkelaar zorg ik ervoor mijn applicatie juist met wachtwoorden omgaat en dat tenminste de aanbeveling van OWASP worden opgevolgd, deze staan hier: https://www.owasp.org/index.php/Authenticati		
mens	· Onvoldoende kennis/training	j	M	M	M M	j	Dit is inderdaad een probleem bij iets nieuws. Alle producten en oplossingen moeten handleidingen en training aanbieden / opleveren voor eindgebruikers. Ontwikkelaars moeten voldoende opgeleid zijn.	Als ontwikkelaar maak ik voor al mijn producten voldoende documentatie zodat eindgebruikers goede handleidingen hebben voor het gebruik van het product in hun situatie.	Als eindgebruiker wil ik opgeleid worden in het gebruik / beheer van de producten en diensten zodat ik in staat ben deze goed te gebruiken en de kans op fouten verminderd.	Als CG organisatie eisen we dat voor producten die ontwikkeld worden tenminste handleidingen en cursusmateriaal mee ontwikkeld wordt zodat eindgebruikers van CG producten opgeleid en begeleid kunnen worden. Daarnaast zorgt dit voor een hogere acceptatie van de producten die we opleveren.

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
mens	**Opzettelijk foutief handelen:**	n					Deels Out of scope, ga er niet van uit dat ontwikkelaars opzettelijk niet volgens voorschriften of procedures werken.			
mens	· Niet werken volgens voorschriften/procedures	J	H	L	H L	j	Ontwikkelaars moeten procedures volgen en onderwezen worden om te voorkomen dat software foutief gemaakt wordt en niet vrij is van fouten. Eindgebruikers moeten worden gedwongen procedures te volgen. De schade van niet volgen voorschriften en procedures kan hoog zijn en de kans laag.	Werken volgens procedures en standaarden Gebruik maken van VWE en CVE lijsten Als ontwikkelaar werk ik volgens moderne standaarden en zorg ik ervoor dat zoveel mogelijk bekende software zwakheden worden voorkomen in de producten die ik maak. Als ontwikkelaar maak ik software die het mogelijk maakt om opzettelijk foutief handelen	Als eindgebruiker wil ik dat opzettelijk foutief handelen wordt voorkomen door invoer controles en achteraf kan worden gedetecteerd door middel van logging	Als CG wil ik dat alle software die wordt gemaakt wordt getest en gepentest waarbij gefocust wordt op het voorkomen van opzettelijke fouten van de programmatuur en de eindgebruiker. Als CG organisatie wil ik dat opzettelijk foutief handelen achteraf kan worden gedetecteerd door middel van logging
mens	· Fraude/diefstal/lekken van informatie	n								
mens	· Ongeautoriseerde toegang met account van medewerker met hogere autorisaties	n								
Apparatuur	**Spontaan technisch falen:**	n					Apparatuur is out of scope Niet van toepassing is van de gemeente zelf in deze eerste risicoanalyse. Indien er centrale CG voorzieningen komen dient er alsnog een aanvullening gemaakt te worden op deze risicoanalyse of in een nieuwe risicoanalyse zodat aanvullende Apparatuur eisen kunnen worden opgenomen in een PvE.	out of scope		De CG organisatie zorgt dat storingen niet (of zo min mogelijk) van invloed zijn op het functioneren van voorzieningen bij gemeenten zodat de dienstverlening van gemeenten kan worden gecontinueerd.
· Functioneert onjuist · Stoort · Gaat verloren of raakt ernstig beschadigd	· Veroudering/slijtage · Storing · Ontwerp/fabricage/installatie-onderhoud fouten	n n n								
	Technisch falen door externe invloeden:	n					Technisch falen is out of scope			
	· Stroomuitval	n								
	· Slechte klimaatbeheersing	n								
	· Nalatig onderhoud door schoonmaak	n								
	· Natuurgeweld	n								
	· Diefstal/schade	n								
	Menselijk handelen/falen:	n					Menselijk handelen met apparatuur is out of scope, geldt later wel voor de beheerfase bij de gemeenten			
	· Installatiefout	n						Als Ontwikkelaar draag ik zorg voor het documenteren en testen van mijn opgeleverde producten op de hardware die voorzien is.	Als beheerder die software beheert voor de eindgebruiker wil ik dat de producten die ik moet installeren op hardware voorzien zijn van duidelijke handleidingen.	De CG organisatie zorgt dat software vooraf (ook geautomatiseerd) is getest en geautomatiseerd wordt gedeployed zodat de kans op fouten tgv menselijke handelingen uitgesloten.
	· Verkeerde instellingen	n								
	· Bedieningsfouten	n								
	· Opzettelijke aanpassingen/sabotage	n								
	· Beschadiging/vernieling	n								

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
	· Verlies/diefstal (onder andere. verlies USB-sticks of andere gegevensdragers)	n								
Apparatuur	· Verwijdering van onderdelen waardoor storingen ontstaan	n								
Programmatuur	**Nalatig menselijk handelen:**	j								
· Functioneert onjuist · Loopt vast of vertraagde uitvoering · Gaat verloren of raakt ernstig beschadigd	· Ontwerp-, programmeer-, invoering, beheer/onderhoudsfouten	j	H	M	H M	j	Schade wordt als hoog ingeschat en kans medium. De schade en vertrouwen van CG is geschaad als er in de producten deze fouten voorkomen, voor de eindgebruiker leidt dit tot niet accepteren van het product of dienst van CG. Voor de fase in beheer leidt dit tot schade voor de betreffende gemeente.	Als ontwikkelaar / bouwer / leverancier maak ik software die het proces ondersteund zoals het bedoeld is en vrij is van fouten en die goed beheerd kan worden. Als ontwikkelaar ontwikkel ik applicaties die waar zo min mogelijk bekende fouten in voor kunnen komen door gebruik te maken van standaard lijsten als de OWASP top 20, CVE lijsten en de MITRE lijst (https://cwe.mitre.org/) Als tester test ik software producten niet alleen functioneel maar ook op bekende software programeer fouten zoals de OWASP top 20, CWE lijst om aan te kunnen tonen dat software zoveel als mogelijk vrij is van bekende fouten en zwakheden Als architect lever ik ontwerpen die duidelijk en begrijpelijk zijn zodat de kans op fouten in het ontwikkel en beheertraject worden verkleind	Als eindgebruiker van CG software producten verwacht ik dat software die ik ga krijgen zoveel als mogelijk vrij is van fouten Als eindgebruiker van CG producten verwacht ik duidelijke gebruikers en beheer handleidingen zodat de producten kunnen worden gebruikt en makkelijk kan worden beheerd.	De CG organisatie zorgt voor verbeteren governance door middel van vaststellen ontwikkelstandaarden, het inrichten van een architectuurfunctie en vaststellen van test/acceptatiecriteria
Programmatuur	· Introductie van virus en dergelijke. door gebruik van niet gescreende programma's	j	H	L	H L	j	Is zaak van de eindgebruikers, bij gebruik Ontwikkelaars mogen alleen tools en bibliotheken gebruiken uit vertrouwde bron	Als ontwikkelaar maak ik bij voorkeur gebruik van gescreende programma's en bibliotheken om de kans om malware zoveel als mogelijk te beperken. Als ontwikkelaar draag ik zorg voor het signen van de software die opgeleverd wordt zodat afnemers kunnen controleren dat de software authentiek is. (? of hashen) Ontwikkelaars maken programma's die goed kunnen performen op de infrastructuur eisen van de gemeente		Als CG organisatie maken we beveiligingsbeleid waarin is vastgelegd dat programma's en bibliotheken uit vertrouwde bron gebruikt moeten worden. Als CG organisatie wil ik dat ontwikkelaars en bedrijven gebruik maken van anti malware programma's en vertrouwde bibliotheken
Programmatuur	· Gebruik van de verkeerde versie van programmatuur	j	M	M	M M	j	Door foutief versiebeheer is de kans groot dat er verkeerder versies van de software en documentatie in omloop zijn met als gevolg schade voor het project en op termijn voor de eindgebruikers van de producten	Als ontwikkelaar draag ik zorg voor juist versiebeheer zodat de kans op fouten wordt verkleind en onderhoud mogelijk wordt.	Als eindgebruiker/beheerder moet ik kunnen toetsen met welke software versie ik werk zodat ik kan vaststellen of de versie juist is en zodat ik dit kan doorgeven aan de helpdesk als er een probleem is.	Als CG organisatie inregelen of laten regelen dat versiebeheer en procedures voor ontwikkelaars van CG om zeker te stellen dat versiebeheer in control komt. Van leveranciers wordt dit vanzelfsprekend verwacht als onderdeel van hun kwaliteitssysteem

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
Programmatuur	· Slechte documentatie	j	M	M	M M	j	Ontwikkelaars hebben broertje dood aan documenteren, zonder documentatie kunnen producten niet gebruikt en beheerd worden door gemeenten en loopt de continuïteit van het ontwikkelproces gevaar. Alle CG ontwikkelaars en projecten moeten gevalideerde en juiste documentatie opleveren	Als ontwikkelaar maak ik gereviewde documentatie voor al mijn producten zodat eindgebruikers en beheerders deze producten kunnen gebruiken en beheren. Ik lever ten minste de volgende documenten (opnemen in acceptatie criteria, definition of done) Denk bijvoorbeeld aan: functionele documentatie Technische documentatie Beheerhandleidingen Gebruikershandleidingen Opleidingsmateriaal Ook op te nemen in de definition of done: documentatie wordt gereviewd door de stakeholder die het betreft	Als eindgebruiker wil ik dat ik geholpen wordt met goede documentatie die mij ondersteund met het juist gebruiken van de software zodat de kans op fouten verkleind wordt	Als CG organisatie willen wij dat alle CG producten van goede kwaliteit zijn, dat geldt ook voor documentatie, daarom willen wij dat er een sluitend QA proces wordt ingericht zodat de documentatie die we aan de gemeenten leveren van goede kwaliteit zal zijn Als CG organisatie wil ik goede documentatie voor het inregelen of laten regelen van de doorontwikkeling, het onderhoud en het beheer, opdat de continuïteit geborgd is en de kans op fouten klein is
Programmatuur	**Onopzettelijk menselijk handelen:**	j				x				
Programmatuur	· Fouten door niet juist volgen van procedures	j	M	L	M L	j	Het niet volgen van procedures leidt tot fouten in de software en onbruikbare producten. Dit leidt tot schade voor CG en de gemeenten. Ontwikkelaars moeten procedures volgen en onderwezen worden. Dit slaat niet op eindgebruikers	Als ontwikkelaar werk ik volgens moderne standaarden en vastgestelde procedures en zorg ik ervoor dat zoveel mogelijk bekende software zwakheden worden voorkomen in de producten die ik maak, hiervoor gebruik ik OWASP, CWE waar dat nodig is.	Als eindgebruiker wil ik dat de software die voor mij gebouwd wordt mij ondersteund in het voorkomen van fouten door middel van duidelijke helpteksten, invoercontroles en duidelijke documentatie	Als CG organisatie zorgen wij voor het vaststellen van procedures en richtlijnen die gebruikt moeten worden bij het ontwikkelen van software. Denk hier aan versiebeheer, en oplever en in beheer name richtlijnen en gebruikers en beheerdocumentatie
Programmatuur	· Installatie van malware en virussen door gebruik van onjuiste autorisaties	j	L	L	L L		Het lijkt me dat ontwikkelaars redelijk bewust zijn. Dit slaat niet op eindgebruikers	Als ontwikkelaar maak ik gebruik van bibliotheken tooling die uit vertrouwde bron afkomstig is zodat de kans op malware en virussen wordt verkleind Als ontwikkelaar zorg ik ervoor dat in mijn producten verschillende autorisatieniveaus zijn zodat rechten voor verschillende typen gebruikers gegeven kunnen worden en maak dit controleerbaar door logging. eis: normale eindgebruikers mogen geen rechten kunnen verwerven waardoor gevaarlijke handelingen kunnen worden uitgevoerd in de software.	is aan de gemeente	
Programmatuur	**Opzettelijk menselijk handelen:**	j								
Programmatuur	· Manipulatie voor of na ingebruikname	j	M	L	M L	j			Als eindgebruiker wil ik dat software die voor mij gebouwd wordt gecontroleerd kan worden op juistheid en onveranderd zijn door bijvoorbeeld code signing of hashing zodat ik zeker weet dat ik met de juiste versie werk	Als common ground dragen we zorg voor een ontwikkelomgeving die ons in staat stelt de kwaliteit van de software te garanderen naar de afnemers
Programmatuur	· (Ongeautoriseerde) functieverandering en/of toevoeging	j	M	L	M L	j		Als ontwikkelaar wil ik dat mijn producten beschermd zijn tegen manipulatie door codesigning en hashing en versioning. Als ontwikkelaar maak ik gebruik van tooling die er voor zorgt dat ongeautoriseerde wijzigingen kunnen worden ontdekt	Als eindgebruiker wil ik dat de software die ik gebruik het mogelijk maakt dat ongeautoriseerde wijzigingen kunnen worden ontdekt door middel van audit logging	Als CG organisatie willen wij dat ongeautoriseerde functieverandering en of toevoeging niet mogelijk door gebruik van ontwikkeltools, codesigning en hashing en het inrichten van wijzigingsbeheer.

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
Programmatuur	· Installatie van virussen, Trojaanse paarden en dergelijke	j	H	L	H L	j		Als ontwikkelaar maak ik gebruik van goedgekeurde bibliotheken om de kans op ingebouwde malware te verkleinen Als ontwikkelaar laat ik mijn producten testen/code reviewen waarbij ook aandacht is voor malware	Als eindgebruiker wil ik alleen software gaan gebruiken die vrij is van malware door middel van acceptatietesten pentesten en gebruiken van geautoriseerde vertrouwde software.	Als CG willen wij de kans op malware verkleinen door het verplichten van antimalware maatregelen bij CG ontwikkelaars en bedrijven.
Programmatuur	· Kapen van autorisaties van collega's	j	H	L	H L	j	Is eigenlijk alleen van belang in de gemeente eindgebruiker situatie. Binnen CG niet direct een issue	Als ontwikkelaar zorg ik ervoor mijn applicatie juist met authenticatie en autorisatie omgaat en dat tenminste de aanbeveling van OWASP worden opgevolgd, deze staan hier: https://www.owasp.org/index.php/Authentication_Cheat_Sheet		
Programmatuur	· Illegaal kopiëren van programmatuur	j				j	Out of scope voor eindgebruikers en ontwikkelen			Als CG organisatie waken we voor het invoeren of omgaan met open source programmatuur met een niet geschikt licentiemodel waardoor deze niet hergebruikt of gebruikt kan worden
Programmatuur	· Oneigenlijk gebruik of privégebruik van bedrijfs-programmatuur	n					Out of scope			
Programmatuur	**Technische fouten/mankementen:**	j								
Programmatuur	· Fouten in code programmatuur die de werking verstoren	j	H	M	H M	j	Grote gevolgen voor heel CG	Als tester test ik software producten niet alleen functioneel maar ook op bekende software programeer fouten zoals de OWASP top 20, CWE lijst om aan te kunnen tonen dat software zoveel als mogelijk vrij is van bekende fouten en zwakheden. Bij testen wordt niet alleen de happy flow getest maar ook gebruik gemaakt van "abuse stories"	Als eindgebruiker van de software verwacht ik dat alle software die CG oplevert uitvoerig is getest op bekende fouten maar ook op onbedoeld gebruik.	Als CG willen we bij kritieke applicaties en kernkomponenten een code review laten uitvoeren om er zeker van te zijn dat geen fouten in de code programmatuur zit. Als CG willen we bij kritieke applicaties en kernkomponenten een software architectuur review laten uitvoeren om vast te stellen dat binnen architectuur standaarden en afspraken gewerkt wordt.
Programmatuur	· Achterdeuren in programmatuur voor (onbevoegde) toegang	j	M	L	M L	j	Dit is zeker een issue dat ook regelmatig het nieuws haalt, kan deels ondervangen worden door testen maar ook opvoeden programmeurs die soms dit doen voor fout opsporing	Als ontwikkelaar draag ik zorg voor het niet ontwikkelen en gebruiken van achterdeurtjes in de code / software die ik oplever		
Programmatuur	· Bugs/fouten in code die tot exploits kunnen leiden	j	H	M	H M	j		Als ontwikkelaar ontwikkel ik applicaties die waar zo min mogelijk bekende fouten in voor kunnen komen door gebruik te maken van standaard lijsten als de OWASP top 20, CVE lijsten en de MITRE lijst (https://cwe.mitre.org/) Als tester test ik software producten niet alleen functioneel maar ook op bekende software programeer fouten zoals de OWASP top 20, CWE lijst om aan te kunnen tonen dat software zoveel als mogelijk vrij is van bekende fouten en zwakheden		De CG organisatie zorgt voor verbeteren governance door middel van vaststellen ontwikkelstandaarden, het inrichten van een architectuurfunctie en vaststellen van test/acceptatiecriteria
Programmatuur	**Organisatorische fouten:**	j								

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
Programmatuur	· Leverancier gaat failliet	j	M	L	M L	j	Risico bestaat altijd en de kans lijkt laag			Als CG laten we bij het ontwikkelen van software door leveranciers/onderaannemers/inhuur voldoende waarborgen inbouwen om de beschikbaarheid van de software ontwikkelproducten te garanderen zoals het afsluiten van een ESCROW overeenkomst of het publiceren als
Programmatuur	· Geen goede afspraken met leverancier	j	M	L	M L	j	Dit risico bestaat en slaat ook op het niet gebben van goede afspraken over licentiemodellen, open source beperkingen etc.			Als CG organisatie gebruiken wij GIBIT of vergelijkbare inkoop voorwaarden om de kans kleiner te maken dat we dingen vergeten als we iets inkopen. We hanteren inkoop procedures
Gegevens	**Via gegevensdragers (CD/DVD/ USB-sticks/ Harddisk/ Back-ups/ mobiele apparaten):**	j					Privacy inbreuk burgers benoemen			
· Worden onterecht ontsloten · Zijn tijdelijk ontoegankelijk · Gaan verloren	· Diefstal/zoekraken/lekken	j	H	M	H M	J	Gegevens mogen niet onterecht ontsloten worden, dit betekent een datalek en dat mag gewoon niet gebeuren dit geldt voor alle toestanden waaronder gegevens zich bevinden van de applicatie. In een omgeving als CG waar veel data op één plek is neemt de kans toe dat dit zou kunnen gebeuren. De schade is dan hoog.	Als een architect / ontwikkelaar wil ik er zeker van zijn dat dat schade aan gegevens en het systeem wordt beperkt als een niet geautoriseerde actor toegang kan krijgen tot een proces of gegevens en daarmee in staat is zich toegang te verschaffen tot gegevens of deze gegevens kan verwijderen.	Als eindgebruiker moet ik er zeker van zijn dat data niet onterecht ontsloten wordt, ik wil duidelijke authenticatie en autorisatie in de applicatie en juiste afhandeling in het systeem. Daarnaast worden de gebruikers en beheerder activiteiten gelogd: zie BIO: 12.4.1 Als eindgebruiker wil ik er zeker van zijn dat data en in het bijzonder persoonsgegevens en bijzondere persoonsgegevens die getransporteerd wordt door de applicatie worden versleuteld.	
Gegevens	· Beschadiging door verkeerde behandeling	j	L	L	L L	N				
Gegevens	· Niet overeenkomende bestandformaten	j	L	L	L L	N				
Gegevens	· Foutieve of geen versleuteling	j	H	M	H M	J	Gegevens mogen niet onterecht ontsloten worden, dit betekent een datalek en dat mag gewoon niet gebeuren dit geldt voor alle toestanden waarin gegevens zich bevinden van de applicatie. In een omgeving als CG waar veel data op één plek is neemt de kans toe	Als ontwikkelaar zorg ik ervoor dat de producten die ik maak in staat zijn gevoelige gegevens te versleutelen (tijdens transport en opslag), ik maak gebruik van algemeen aanvaarde goede encryptie technieken		**Als CG organisatie beschrijven we welke vormen van versleuteling we wanneer verplicht stellen zodat er duidelijkheid is voor betrokkenen en toetsing mogelijk is.**
Gegevens	· Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen	n								
Gegevens	**Via Cloud voorzieningen:**	j								

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
Gegevens	· Ongeautoriseerde toegang door onbevoegden (hackers/hosters)	j	H	M	H M	j	Het is de verwachting dat delen van Common Ground software als cloudapplicatie zullen worden gebruikt, hierdoor nemen specifieke Cloud risico's toe.	Als ontwikkelaar van CG software producten zorg ik ervoor dat alle software getest is en webfacing software moet een pentest ondergaan.	Als eindgebruiker van de software verwacht ik dat alle software die CG oplevert uitvoerig is getest en gepentest op bekende fouten maar ook op onbedoeld gebruik. Als eindgebruiker / gemeente wil ik dat software die we gaan gebruiken in de Cloud is getest en gepentest om zoveel als mogelijk ongeautoriseerde toegang door Hackers uit te sluiten. Als eindgebruiker / gemeente wil ik dat software die binnen de gemeente of buiten de gemeente in de Cloud draait wordt gemonitord op ongeautoriseerde toegang door onbevoegde door middel van een SIEM oplossing en een SOC zodat ik tijdig waarschuwingen krijg	Als CG organisatie hebben we de verantwoordelijkheid om fatsoenlijk om te gaan met broncodes van software en testgegevens. Wij richten processen in om er voor te zorgen dat er geen ongeautoriseerde toegang tot broncode is. In het geval van GitHub / open source zorgen we controle van broncode en testen.
gegevens	· Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)	j	H	M	H M	j	Hacking is altijd een risico en zeker met Cloud systemen en webbased systemen als ook Internet in het spel is. De schade kan zeer hoog zijn en de kans medium.	Als ontwikkelaar maak ik CG software producten die het mogelijk maken dat fouten kunnen worden hersteld door middel van back-up en restore, rollback strategieën en logging	Als eindgebruiker / gemeente wil ik dat de software die door de leverancier wordt geleverd mij in staat stelt om ongeautoriseerde wijzigingen te kunnen ontdekken door logging en log controle en dat ongeautoriseerde wijzigingen kunnen worden hersteld door middel van back-up en restore of andere roll back mechanismes	Als CG organisatie zorgen wij ervoor dat de toegang tot software en software broncode wordt gecontroleerd. Als CG organisatie zorgen wij ervoor dat ongeautoriseerde wijzigingen in software kunnen worden hersteld door versiebeheer procedures en back-up en restore.
Gegevens	**Via apparatuur:** · Fysieke schrijf- of leesfouten · Onvoldoende toegangsbeperking tot apparatuur · Fouten in interne geheugens · Aftappen van gegevens	n n n n n					Is voor de gemeente			
Gegevens	**Via programmatuur:** · Foutieve of gemanipuleerde programmatuur	j j	H	L	H L	j	Kans is laag en schade kan hoog zijn, gemanipuleerde en foutieve programmatuur is een redelijk risico voor de einsgebruiker en voor CG als geheel.		Als eindgebruiker wil ik software die vrij is van fouten en die van te voren is getest op bekende zwakheden en programmeerfouten.	Als CG organisatie zorgen we voor een kwaliteitsborging om de producten van CG van goede kwaliteit te laten zijn. Bijvoorbeeld door testen en/of code reviews
	· Doorwerking van virussen/malware	j	L	L	L L		Is een risico maar meer voor de gemeente			
	· Afbreken van verwerking	j	M	L	M L	j	Is een risico wordt als midden en kans laag ingeschat	Als ontwikkelaar maak ik software die in staat is om afbreken van verwerking te herstellen zodat de eindgebruiker geen gegevens verliest. Als dit niet kan zorg ik voor duidelijke herstelboodschappen zodat schade verder beperkt kan worden	Als eindgebruiker van een CG product wil ik bij afbreken van verwerking geen gegevens kwijt zijn en als dat niet lukt een duidelijke aanwijzing over herstelmogelijkheden.	
Gegevens	**Via personen:**	j								

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
	· (On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data	j	H	L	H L		Onopzettelijke foutieve gegevensinvoer, - verandering of verwijdering van data kan leiden tot hoge schade voor de gemeente en de burger.	Als ontwikkelaar van CG applicaties zorg ik ervoor dat maatregelen worden genomen in mijn applicaties om (on)opzettelijke foutieve gegevensinvoer en -verandering en -verwijdering tegen te gaan door het bouwen van mogelijkheden voor fouten afvangen, back-up, integriteits controle invoer, logging en monitoring voor herstel achteraf.	Als eindgebruiker van een CG product wil ik dat juiste gegevensinvoer wordt afgedwongen en tevens dat het veranderen of verwijderen van gegevens moet worden bevestigd alvorens door te gaan. Als eindgebruiker en functioneel beheerder wil ik dat foutieve gegevensinvoer . verandering of verwijdering kan worden gedetecteerd en gelogd zodat herstel mogelijk is achteraf.	
gegevens	· Onbevoegde toegang door onbevoegden	j	H	L	H L		Onbevoegde toegang tot de (persoons) gegevens verwerkende systemen van de gemeente leidt direct tot een datalek waarmee de AVG wordt overtreden. Los daarvan kan dit leiden tot schade voor de gemeente en de burger	Als ontwikkelaar/architect van CG producten zorg ik dat authenticatie en autorisatie worden ingericht in de producten/applicaties die ik maak, zodanig dat onbevoegde geen toegang kunnen krijgen tot gegevens waar zij niet bij mogen komen. Als ontwikkelaar / architect zorg ik ervoor dat in CG producten waar gewerkt wordt met (bijzondere) persoonsgegevens alleen toegang verkregen kan worden middels gebruikersnaam en wachtwoord, bij toegang vanuit een andere zone wordt uitsluitend toegang verleend door middel van 2FA middels een centrale component. Als ontwikkelaar / architect sluit ik aan bij de Common Ground API strategie voor wat betreft autorisatie en beveiligingseisen die op API's van toepassing zijn. Als ontwikkelaar / architect zorg ik ervoor dat alle geslaagde en niet geslaagde inlogpogingen en toegang tot informatie worden gelogd door de applicatie Als ontwikkelaar / architect zorg ik ervoor dat alle geslaagde en niet geslaagde inlogpogingen en toegang tot informatie van beheerders worden gelogd door de applicatie	Als eindgebruiker van een CG product wil ik dat er voldoende mechanismes zijn geïmplementeerd om onbevoegde toegang door onbevoegden te voorkomen.	Als CG organisatie beschrijven we welke authenticatie en autorisatiemechanismen zijn toegestaan voor gebruikers en applicaties zodat….
gegevens	· Onbevoegd kopiëren van gegevens	j	H	L	H L	J	De schade van onbevoegd kopiëren is altijd hoog, de kans dat een ambtenaar dit doet wordt als laag ingeschat. Van onbevoegden moet worden voorkomen dat ze dit kunnen. IS voor de gemeente belangrijk ook in andere situaties		Als proces-/systeemeigenaar wil ik dat het kopiëren van gegevens kan worden gedetecteerd en gelogd zodat ik daar achteraf controle op kan uitvoeren	
	· Meekijken over de schouder door onbevoegden	n					Is voor de gemeente een issue			

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
	· Onzorgvuldige vernietiging	n					Is voor de gemeente belangrijk, en dit is voor Cloud voorzieningen zeker belangrijk. De gemeente regelt dit in een verwerkersovereenkomst, contract, SLA o.i.d. op basis van de gegevens classificatie			Als Cg organisatie zorgen we voor afspraken over vernietiging van data als we applicaties integraal inkopen/beheren voor gemeenten
	· Niet toepassen clear screen/clear desk	n					Is voor de gemeente een issue			
	· Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties)	n					Is voor de gemeente een issue			
	· Oneigenlijk gebruik van autorisaties	n					Is voor de gemeente een issue			
	· Toegang verschaffen tot gegevens door middel van identiteitsfraude of social engineering	n					Is voor de gemeente een issue			
Organisatie	**Gebruikersorganisatie:**	j								
· Werkt niet volgens vastgestelde uitgangspunten	· Mismanagement	n				j	CG risico			
· Reorganiseert										
· Fuseert of wordt opgeheven										
	· Gebrekkige toedeling taken, bevoegdheden, verantwoordelijkheden	j	M	L	M L	j	CG risico			
	· Onduidelijke of ontbrekende gedragscodes	n					CG risico			
	· Afwezige, verouderde of onduidelijke handboeken /systeemdocumentatie / werkprocedures/ gebruiksinstructies	j	M	M	M M	j	eindgebruiker en CG risico, zeker omdat er in veel verschillende teams of bij veel verschillende partijen kan worden ontwikkeld is de kans schade medium en de kans ook. Het is dus zorg hier aandacht voor te hebben en daarmee de kans en mogelijke schade te verlagen	Als ontwikkelaar draag ik zorg voor het documenteren van de producten die ik moet opleveren, als criteria gebruik ik de acceptatie criteria van CG bij de definition of done	Als eindgebruiker wil ik dat de opgeleverde producten die ik ga gebruiken voldoende documentatie hebben zodat ik in staat ben te begrijpen hoe het systeem werkt en ik minder fouten maak.	Als Common Ground wil ik dat alle opgeleverde producten die in beheer worden genomen voldoen aan vooraf vastgestelde acceptatie criteria Als CG organisatie wil ik dat er acceptatie criteria zijn vastgesteld per productsoort die in ieder geval getoetst worden bij overdracht naar beheer.
	· Onvoldoende interne controle	j	M	L	M L		CG risico			
	· Onvoldoende toetsing op richtlijnen	j	M	L	M L		CG risico			
	· Onvoldoende of geen contractbeheer	j	M	L	M L		CG risico			
	· Ontbrekende of onduidelijke SLA's	j	M	L	M L		CG risico			
	· Gebrekkige doel/middelen beheersing	j	M	L	M L		Cg risico			
	Beheerorganisatie:	j								
	· Gebrekkig beleid betreffende beheer	j	H	L	H L		CG en gemeente risico			
	· Onvoldoende kennis of capaciteit	j	M	M	M M		CG en gemeente risico			
	· Onvoldoende kwaliteitsborging	j	H	M	H M		CG risico			
	· Onvoldoende beheer van systemen en middelen	j	H	M	H M		CG risico			
	Ontwikkelingsorganisatie:	j								
	· Slecht projectmanagement	j	M	L	M L		CG risico			
	· Niet volgen van projectenkalender of PPM	j	M	L	M L		CG risico			
	· Geen ontwikkelrichtlijnen en/of – procedures	j	H	M	H M		CG risico			
	· Er worden geen methoden/technieken gebruikt	j	H	M	H M		CG risico			

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
	· Gebrek aan planmatig werken	j	M	M	M M		CG risico			
Omgeving · Is toegankelijk voor ongeautoriseerden · Is beschadigd · Is verwoest of ernstig beschadigd **omgeving**	**Huisvesting:** · Ongeautoriseerde toegang tot gebouw(en) · Diefstal op werkplekken · Gebreken in ruimtes, waardoor kans op insluiping/inbraak · Onvoldoende fysieke voorzieningen om te vluchten of in te grijpen tijdens geweldsdreigingen/conflicten met klanten	n n n n n					Fysiek (omgeving) is buiten scope gemeente risico gemeente risico gemeente risico gemeente risico			
	Nutsvoorzieningen: · Uitval van elektriciteit, water, telefoon · Wateroverlast door lekkage, bluswater · Uitval van licht-, klimaat- en sprinklerinstallatie	n n n n					Out of scope gemeente risico gemeente risico gemeente risico			
	Buitengebeuren: · Natuurgeweld (overstroming, blikseminslag, storm, aardbeving et cetera) · Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig) · Blokkade/staking · Onveilige, geblokkeerde, vluchtwegen bij brand	n n n n n					Out of scope gemeente risico gemeente risico gemeente risico gemeente risico			
Diensten · Worden niet volgens afspraak geleverd · Tijdelijk niet te leveren · Definitief niet meer te leveren	**Diensten worden niet conform afspraak geleverd:** · Slecht opgeleid personeel · Groot personeelsverloop · Onvoldoende capaciteit in personeel · Valse verklaringen over certificeringen · Onvoldoende of geen kwaliteitsborging · Personeel voldoet niet aan eisen zoals een geldige VOG en getekende geheimhoudingsverklaringen · Voert wanbeheer, slordigheden in beheersactiviteiten,	j j j j n j n j	M M H H H	L L H M L	M L M L H H H M H L	 j j	 Out of scope, ondervangen door inhuur Out of scope, ondervangen door inhuur Dit is een hoog risico dat er onvoldoende capaciteit en kwaliteit beschikbaar is en blijft, met name voor gemeenten. Out of scope Onvoldoende kwaliteitsborging zorgt voor producten voor common ground die niet geschikt zijn voor gemeenten Out of scope, zit in inhuur regels VNG Gedurende de looptijd van CG bestaat het risico dat op de lange termijn grote schade kan ontstaan door foutief beheer met als gevolg dat deelnemers daar schade van ondervinden. Dit slaat op CG zelf en ook leveranciers van software producten			 Als CG organisatie zorgen we voor een vaste kern van zeer deskundige medewerkers op het gebied van softwareontwikkeling en deployment om kwaliteit en continuïteit te garanderen. Als CG organisatie willen wij dat producten goed in beheer worden genomen en blijven met als doel het langdurig in stand houden van producten en diensten van CG. Er moet aandacht zijn voor beheeractiviteiten bij alle partijen.

Component	Incident	scope RA?	(L,M,H) Schade	(L,M,H) Kans	(L,M,H) Totaal	Scope maat-regel	Toelichting (gevolgen et cetera)	Ontwikkelaar Userstory	user NF Userstory	CG organisatie userstory
Diensten	· Werkt niet conform ITIL of BiSL principes	n								
	· Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie	n								
	· Houdt zich niet aan functiescheiding	n								
	· Maakt gebruik van te zware autorisatie, niet functie gebonden	j	H	M	H M	j	Software voor CG moet mogelijkheden bevatten om dit tegen te gaan of te ontdekken omdat onjuiste autorisatie leid tot datalekken en misbruik van processen. Dit is meer iets voor de gemeente die autorisaties periodiek moet controleren, de software moet dit dan wel makkelijk ondersteunen		Als eindgebruiker/proceseigenaar wil ik dat het mogelijk is om periodiek autorisaties te beoordelen op het scherm en/of print zodat ik de mogelijkheid heb om deze controletaak uit te voeren. Als functioneel beheerder wil ik door de software gewaarschuwd worden bij het instellen van conflicterende en/of te zware autorisaties in de systemen die ik gebruik.	
Diensten	**Diensten dienstverlener tijdelijk niet beschikbaar:**	**j**								
	· Levert diensten niet conform overeenkomst	j	H	M	H M	j	Producten die voor CG geleverd worden moeten volgens overeenkomst worden geleverd omdat anders de kans groot is dat producten worden geleverd om mogelijk niet geschikt zijn voor gebruik door gemeenten. Zonder overeenkomst is de schade hoog en de kans midden			Als CG organisatie worden producten die uitgevraagd worden duidelijk gespecificeerd met een PVE waarin ook security non functionals worden meegenomen. Deze documenten worden gebruikt voor kwaliteitscontrole en testen bij oplevering. Daarnaast hanteren wij duidelijke in beheer name criteria als wij zelf deze producten gaan beheren.
	· Onderbreking dienstverlening door overname dienstverlener	n					Out of scope			
	· Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen en dergelijke)	n					Out of scope			
	· Past verkeerde prioriteiten toe in klantbejegening	n					Out of scope			
	· Levert onvoldoende capaciteit voor een goede dienstverlening	j	M	L	M L		Op te nemen in overeenkomsten			
Diensten	**Diensten dienstverlener definitief niet meer te leveren:**	n								
	· Een dienstverlener gaat failliet	j	H	L	H L	j	Is een risico als de leverancier software maakt die we vervolgens niet krijgen of die niet meer onderhouden kan worden			Als CG organisatie sluiten we met leveranciers die mogelijk dit risico hebben een escrow overeenkomst af als onderdeel van de contracten met die leveranciers. Zie Gibit
	· Opzegging diensten door dienstverlener	j	M	L	M L		Is een medium schade, lage kans omdat als dit gebeurt we op zoek moeten naar een andere leverancier voor bestaande functionaliteit, meestal zie je dit wel aankomen en kun je anticiperen. Geen userstory			

		SCHADE		
		H	**M**	**L**
KANS	**H**	HH	HM	HL
	M	MH	MM	ML
	L	LH	LM	LL

Bijlage D: Dreigingen specifiek voor soorten informatiesystemen

Om de uitvoering van de dreigingsanalyse efficiënter en effectiever te laten verlopen, kan gebruik gemaakt worden van van te voren vastgestelde dreigingen die expliciet relevant zijn voor het onderhavige informatiesysteem. Deze bijlage beschrijft een aantal soorten informatiesystemen met de bijbehorende

De voor ingevulde lijst met dreigingen bevat alleen de algemene dreigingen. Uit onderstaande lijst worden potentiele dreigingen toegevoegd (zie hoofdstuk 3, stap 1, punt 2 de beschrijving van de stappen) aan de te bespreken lijst. Door in deze tabel voorbeelden van de meest voorkomende en relevante soorten systemen op te nemen worden de juiste dreigingen toegevoegd. Deze bijlage met dreigingen kan qua systemen en

Deze lijst is eventueel zelf aan te vullen op basis van eigen inschattingen.

Documentair informatiesysteem

- Documenten niet beschikbaar voor proces (grote afhankelijkheid centrale opslag)
- Documenten niet vindbaar wegens bijvoorbeeld onjuiste metagegevens
- Documenten voor niet geautoriseerden zichtbaar wegens onjuiste autorisaties

Via het internet toegankelijk webbased informatiesysteem

- Lekken van gegevens door ‘hacker’
- Defacement van website
- Fraude als gevolg van misbruik van gegevens door ‘hackers’
- Website niet beschikbaar wegens DDoS aanval
- Infectie door oneigenlijke installatie van malware op de site door gebruikers van de website

Basisregistratie/kernregistratie

- Ongewenste verandering van gegevens bij conversie/ophalen gegevens
- Onjuiste invoer van gegevens waardoor onjuistheden ontstaan in andere registraties
- Ongeautoriseerde toegang tot basisregistraties wegens foutieve inrichting
- Niet beschikbaar voor afhankelijke systemen door uitval

Financieel systeem

- Financiële fraude als gevolg van misbruik
- Onvoldoende controle op gebruik
- Ongeautoriseerde toegang tot financiële gegevens

Personeelssysteem

- Onbevoegd inzien door een persoon van gegevens
- Lekken van persoonsgegevens door onjuiste inrichting
- Ongeautoriseerde verwerking van persoonsgegevens

Facilitair systeem

- Onbevoegd toegang verschaffen tot de gemeente
- Onbevoegd gebruik maken van systemen

Ketensysteem

- Systeem niet beschikbaar voor proces/keten
- Onjuiste invoer / wijziging van gegevens waardoor ketenfouten ontstaan
- Onbevoegde toegang tot ketengegevens
- Niet voldoen aan wet- en regelgeving

Systeem in de Cloud

- Niet voldoen aan wet- en regelgeving omdat gegevens in de Cloud staan
- Afhankelijkheid van Cloudleverancier met betrekking tot beschikbaarheid
- Toegangscontrole onvoldoende c.q. onbeheersbaar

Procesondersteuningssysteem

- Procesondersteuning is onjuist waardoor foutieve producten worden geleverd

Systeem obv microservices

- Hoge complexiteit en daardoor niet robuust
- Inconsistentie van data vanwege BASS ipv ACID transacties
- Verstoringen als gevolg van aanpassing van een onderdeel
- Ontbreken van voldoende kennis bij beheer