Bijlage 4

Beschrijving risicoanalysemethode

1. Inleiding

De eerstelijnszorg wordt steeds afhankelijker van de betrouwbaarheid van geautomatiseerde informatiesystemen. Ernstige gevolgen voor de patiëntenzorg of voor de bedrijfsvoering in het algemeen kunnen ontstaan indien:

- Informatie uit systemen onjuist of onvolledig is;
- Informatiesystemen niet beschikbaar zijn;
- Informatie onverhoopt in handen van derden komt die hiertoe niet zijn geautoriseerd.

Vandaar dat het van groot belang is in kaart te brengen wat de risico's zijn als deze informatie om wat voor reden ook niet (juist) voorhanden is. Het is mogelijk een risicoanalyse uit te voeren naar de belangrijkste objecten (systemen).

2. De methode

De risicoanalysemethode bestaat uit de volgende stappen:

1. Identificatie van de objecten van de risicoanalyse (bedrijfsproces, informatiesysteem of informatie);
2. Analyse van het object;
3. Dreigingenanalyse;
4. Bepalen van algemene en specifieke beveiligingsmaatregelen.

De methode kan gebruikt worden voor telefonie, patiëntregistratiesysteem, et cetera (zie ook bijlage 5: Risicoanalyses NEN 7511-2).

2.1 Identificatie van de objecten van de risicoanalyse

De risicoanalyse start met een identificatie van de objecten van de risicoanalyse: bedrijfsproces, informatiesysteem en informatie. Doel is een goed en volledig inzicht te krijgen in elk van deze objecten.

2.2 Analyse van het object van de risicoanalyse

Voor de daadwerkelijke risicoanalyse wordt met behulp van een drietal formulieren bepaald wat de mogelijke gevolgen zijn van het niet betrouwbaar functioneren van het object:

- **Beschikbaarheid**: gaat in op de mogelijke gevolgen voor de patiëntenzorg als het systeem niet beschikbaar is.
- **Integriteit:** gaat in op de mogelijke gevolgen voor de patiëntenzorg wanneer het systeem onjuiste of onvolledige gegevens beschikbaar stelt of wanneer gegevens niet tijdig beschikbaar zijn.
- **Vertrouwelijkheid:** gaat in op de mogelijke gevolgen voor de patiëntenzorg wanneer gegevens uit het systeem in handen komen van derden die hiertoe niet zijn geautoriseerd.

2.3 Dreigingenanalyse

Op basis van een standaardlijst van bedreigingen uit de risicoanalyse worden de relevante bedreigingen voor het object van analyse bepaald. Hierbij wordt gekeken welke bedreigingen het grootste risico vormen voor het object van analyse. Dit kan met behulp van formulieren 4 t/m 6 (zie hieronder). Die gaan in op de dreigingen ten aanzien van

beschikbaarheid, integriteit en vertrouwelijkheid.

2.3.1 Risicoprofiel
Aan de hand van deze risicoanalyse wordt voor ieder geautomatiseerd informatiesysteem bepaald wat het risicoprofiel of zogenaamde BIV-classificatie is (BIV staat voor Beschikbaarheid, Integriteit, Vertrouwelijkheid). Op basis van de BIV-classificatie kan het vereiste beveiligingsniveau voor de applicatie worden bepaald. Een hoge BIV-classificatie leidt tot een hoog vereist beveiligingsniveau en dus tot strikte beveiligingsstandaarden en strenge beveiligingsmaatregelen.

De risicoanalyse wordt uitgevoerd aan de hand van zes formulieren:
Met behulp van de formulieren 1 t/m 3 wordt bepaald wat de mogelijke gevolgen zijn van het niet betrouwbaar functioneren van het systeem. Er wordt antwoord gegeven op de vraag in welke mate de bedrijfsvoering of patiëntenzorg wordt geschaad wanneer het systeem niet betrouwbaar functioneert.

- Formulier 1 gaat in op mogelijke gevolgen voor de bedrijfsvoering of voor de patiëntenzorg wanneer het systeem tijdelijk niet beschikbaar is.
- Formulier 2 gaat in op de mogelijke gevolgen voor de bedrijfsvoering of voor de patiëntenzorg wanneer het systeem onjuiste of onvolledige gegevens beschikbaar stelt of wanneer gegevens niet tijdig beschikbaar zijn.
- Formulier 3 gaat in op de mogelijke gevolgen voor de bedrijfsvoering of voor de patiëntenzorg wanneer gegevens uit het systeem in handen van derden komen die hiertoe niet zijn geautoriseerd.

2.3.2 Formulieren 1 t/m 3 Effecten
Op de eerste drie formulieren wordt u gevraagd een classificatie aan te geven voor de ernst van mogelijke effecten. Hieronder vindt u een omschrijving van de mogelijke classificaties.

Classificatie 5 – Continuïteitsbedreiging
(levensbedreigende situatie)
Het systeem is van kritiek belang voor de bedrijfsvoering, of het systeem is de enige bron van belangrijke gegevens voor de patiëntenzorg. Uitval en fouten kunnen ernstige gevolgen hebben voor de bedrijfsvoering of voor het welzijn van patiënten.

Classificatie 4 – Serieuze schade
(serieuze bedreiging voor het welzijn van de patiënt)
Het systeem is van aanzienlijk belang voor de bedrijfsvoering, of het medisch handelen wordt deels op basis van gegevens uit dit systeem bepaald. Er bestaat een reële kans op schade aan de bedrijfsvoering of aan het welzijn van patiënten bij uitval en fouten.

Classificatie 3 – Behoorlijke schade
(beperkte bedreiging voor het welzijn van de patiënt)
Het systeem is belangrijk voor de bedrijfsvoering, of het systeem is belangrijk voor de patiëntenzorg. Door noodprocedures en/of expertise is de kans op schade aan de bedrijfsvoering of aan het welzijn van patiënten door uitval of fouten echter beperkt.

Classificatie 2 – Minimaal effect
(kans op hinder voor de patiënt)
Er bestaat een kans op hinder voor de bedrijfsvoering of voor patiënten bij uitval van het systeem of bij fouten. Ernstiger schade voor de bedrijfsvoering of voor de

patiëntenzorg is zeer onwaarschijnlijk (veelal administratief ondersteunende systemen).

Classificatie 1 – Te verwaarlozen
(gevolgen voor de patiëntenzorg zijn onwaarschijnlijk)
Directe gevolgen voor de bedrijfsvoering of voor patiënten als gevolg van uitval van het systeem of fouten zijn zeer onwaarschijnlijk (veelal ondersteunende systemen).

Enkele voorbeelden:
Het beantwoorden van de vragen is het eenvoudigst wanneer u als volgt redeneert:

Voorbeelden (B3 = Vraag 3, formulier 1: beschikbaarheid):

B3 : Wanneer de applicatie circa een week niet beschikbaar is, kan dit leiden tot behoorlijke schade (3) omdat wettelijk voorgeschreven of contractuele verplichtingen niet kunnen worden nageleefd.
B6 : Wanneer een applicatie regelmatig ongeveer een dag niet beschikbaar is beïnvloedt dit de moraal van de medewerkers niet en heeft dit een minimaal effect (2) op de patiëntenzorg of op de bedrijfsvoering.
I1 : Wanneer de applicatie onjuiste of onvolledige informatie levert of informatie niet tijdig levert, kan dit leiden tot serieuze bedreiging (4) van het welzijn van de patiënt omdat het risico bestaat dat een verkeerde behandelmethode wordt gekozen.
I2 : Wanneer de applicatie onjuiste of onvolledige informatie levert of informatie niet tijdig oplevert, kan dit leiden tot een continuïteitsbedreiging of een levensbedreigende situatie (5) omdat het management geen gefundeerde beslissingen kan nemen.
V2 : Wanneer vertrouwelijke of gevoelige (financiële) informatie in handen komt van ongeautoriseerden, kan dit leiden tot serieuze schade (4) omdat het welzijn van de patiënt wordt geschaad en hij het vertrouwen in het ziekenhuis verliest.
V3 : Wanneer vertrouwelijke of gevoelige (financiële) informatie in handen komt van ongeautoriseerden, kan dit leiden tot behoorlijke schade (3) omdat wet- en regelgeving (bijvoorbeeld de Wet bescherming persoonsgegevens) wordt overtreden en claims bij de zorginstelling worden ingediend.

2.3.3 Formulieren 4 t/m 6 Kansen
Met behulp van de formulieren 4 t/m 6 wordt bepaald wat de kans is dat bepaalde bedreigingen ten aanzien van de betrouwbaarheid van de applicatie zich voordoen.

- Met behulp van formulier 4 wordt de kans bepaald dat mogelijke bedreigingen ten aanzien van de beschikbaarheid van het systeem zich manifesteren.
- Met behulp van formulier 5 wordt de kans bepaald dat mogelijke bedreigingen ten aanzien van de integriteit (juistheid, volledigheid, tijdigheid) van de gegevens uit het systeem zich manifesteren.
- Met behulp van formulier 6 wordt de kans bepaald dat mogelijke bedreigingen ten aanzien van de vertrouwelijkheid van de gegevens uit het systeem zich manifesteren.

Na het invullen van de formulieren 1 t/m 6 worden de ‘totaalscores’ van deze formulieren overgenomen op het voorblad. Op basis van deze samenvatting is vervolgens de BIV-classificatie te bepalen.

2.4 BIV-classificatie en risicobeheersmaatregelen
De risicoanalyse eindigt met het berekenen van de BIV-classificatie. Hierbij wordt effect vermenigvuldigd met de kans op een bepaalde gebeurtenis. Tezamen bepaalt dit dan het

risico.
Bij een BIV-classificatie in klasse 4 en 5 moeten (in samenspraak met leverancier) maatregelen genomen worden om de risico's te verkleinen.
Bij een BIV-classificatie in de klasse 3 wordt gekeken naar de individuele scores op onderdelen. Als er op bepaalde punten sprake is van score 5 (continuïteitsbedreiging) of een kans van 4 of 5 (hoogstwaarschijnlijk), dan is het zaak te kijken of op deze punten verdere maatregelen genomen dienen te worden. Bij een hoge score voor continuïteitsbedreiging, maar een zeer geringe kans op daadwerkelijk plaatsvinden, is hiervan af te zien.
BIV-classificatie 1 of 2 leidt niet tot extra maatregelen.

3. Uitwerking uitgebreide risicoanalyses

Het verdient aanbeveling de risicoanalyse uit te voeren vanuit het perspectief dat de professionele samenvatting operationeel is. De afhankelijkheid van informatie is dan namelijk groter dan in het verleden.

3.1 Evaluatie en beleid risicoanalyse en methode

De risicoanalysemethode wordt eens in de drie jaar geëvalueerd door de kwaliteitsfunctionaris.
De risicoanalyse wordt jaarlijks geëvalueerd door de systeemeigenaar in samenspraak met de kwaliteitsfunctionaris.
Bij tussentijdse grote wijzigingen (bijvoorbeeld een nieuw systeem, nieuwe relevante releases) kan de evaluatie ook eerder plaatsvinden.

Voorblad risicoanalyse

Organisatieonderdeel/afdeling :
Systeem/applicatie :
Systeemeigenaar : bijvoorbeeld de informatieadviseur
Datum :
Versie/datum laatste wijziging :

Ik ga akkoord met de samenvatting en de BIV-classificatie zoals hieronder aangegeven:

Handtekening systeemeigenaar : _____
Datum: _____

Samenvatting

	Effect	Kans	Risico	Van risico naar BIV-klasse
Beschikbaarheid	B	BB	B x BB	Risico 1 t/m 4 = BIV-klasse 1 Risico 5 t/m 8 = BIV-klasse 2 Risico 9 t/m 12 = BIV-klasse 3 Risico 15 t/m 16= BIV-klasse 4 Risico 20 t/m 25 = BIV-klasse 5
Integriteit	I	BI	I x BI	
Vertrouwelijkheid	V	BV	V x BV	

Toelichting afkortingen:
B : Totaalscore formulier 1: Beschikbaarheid/continuïteit
I : Totaalscore formulier 2: Integriteit
V : Totaalscore formulier 3: Vertrouwelijkheid
BB : Totaalscore formulier 4: Bedreigingen t.a.v. beschikbaarheid/continuïteit
BI : Totaalscore formulier 5: Bedreigingen t.a.v. integriteit
BV : Totaalscore formulier 6: Bedreigingen t.a.v. vertrouwelijkheid

BIV-classificatie

Beschikbaarheid	
Integriteit	
Vertrouwelijkheid	

Conclusie

Geef hier een samenvatting van de bevindingen en de mogelijke verbeteringen.

Formulier 1: Beschikbaarheid/continuïteit

Mogelijke effecten van het (tijdelijk) niet beschikbaar zijn van een applicatie of systeem.		**Classificatie** 5 Continuïteitsbedreiging 4 Serieuze schade 3 Behoorlijke schade 2 Minimaal effect 1 Te verwaarlozen					**Toelichting**
		Uitval tijd					
		1 uur	1 dag	2-3 dagen	1 week	> 1 week	
B1	**Directe schade voor de bedrijfsvoering of patiëntenzorg.** Hoe ernstig zijn de directe gevolgen voor de bedrijfsvoering of voor de patiëntenzorg wanneer de applicatie (regelmatig) niet beschikbaar is voor een bepaalde tijd?						
B2	**Besluitvorming door het management** Wat is het effect op de besluitvorming van het management wanneer de applicatie (regelmatig) niet beschikbaar is voor een bepaalde tijd?						
B3	**Verlies van vertrouwen/ imagoschade** Wat is het effect op het vertrouwen van de patiënt of de reputatie van de organisatie wanneer de applicatie (regelmatig) niet beschikbaar is?						
B4	**Wet- en regelgeving** Wat is het effect op de naleving van wettelijke, voorgeschreven of contractuele verplichtingen wanneer de applicatie (regelmatig) niet beschikbaar is?						
B5	**Herstelkosten** Wat is het effect op de additionele kosten voor het herstellen van een opgelopen achterstand wanneer de applicatie niet (tijdelijk) beschikbaar is geweest?						
B6	**Moraal van de medewerkers** Wat is het effect op de moraal van de medewerkers wanneer de applicatie (regelmatig) niet beschikbaar is?						
B7	**Fraude** Bestaat een risico dat geld of goederen frauduleus worden aangewend wanneer de applicatie (regelmatig) niet beschikbaar is? En wat is hiervan de mogelijke consequentie?						
B8	**Overige risico's** Signaleert u nog andere risico's als gevolg van het (regelmatig, tijdelijk) niet beschikbaar zijn van de applicatie? En wat zijn hiervan de mogelijke consequenties?						
BT	**Totaal** Samenvattend, rekening houdend met de notering hierboven, wat is in het ergste geval het gevolg voor de bedrijfsvoering of de patiëntenzorg wanneer de applicatie uitvalt op het meest ongunstige moment?						
BMU	**Maximale uitvalstijd** Wat is de maximaal toelaatbare periode dat de applicatie niet beschikbaar mag zijn; het overschrijden van deze periode leidt tot onaanvaardbare consequenties voor de bedrijfsvoering of voor de patiëntenzorg.						

Formulier 2: Integriteit (juistheid, volledigheid, tijdigheid)

Mogelijke effecten van niet juiste, volledige of niet tijdige informatie.		**Classificatie** 5 Continuïteitsbedreiging 4 Serieuze schade 3 Behoorlijke schade 2 Minimaal effect 1 Te verwaarlozen					**Toelichting**
I1	**Directe schade voor de bedrijfsvoering of patiëntenzorg.** Hoe ernstig zijn de directe gevolgen voor de bedrijfsvoering of voor de patiëntenzorg wanneer informatie uit dit systeem niet juist, volledig of tijdig is?						
I2	**Besluitvorming door het management** Wat zijn de gevolgen voor de besluitvorming van het management wanneer de informatie uit dit systeem niet juist, volledig of tijdig is?						
I3	**Verlies van vertrouwen** Wat is het mogelijke effect op het vertrouwen van patiënten of de reputatie van de CHN wanneer de informatie uit dit systeem niet juist, volledig of tijdig is?						
I4	**Wet- en regelgeving** Wat is het effect van het mogelijk niet kunnen naleven van wet- en regelgeving als gevolg van het niet juist, volledig of tijdig beschikbaar zijn van informatie uit het systeem?						
I5	**Moraal van de medewerkers** Wat is het effect op de moraal van de medewerkers wanneer de informatie uit het systeem niet juist, volledig of tijdig is?						
I6	**Fraude** Kan frauduleuze aanwending van geld of goederen voortkomen uit of verborgen worden door het ongeautoriseerd muteren van informatie?						
I7	**Additionele kosten** Wat is het mogelijke effect van eventuele additionele kosten die kunnen ontstaan als gevolg van het niet juist, tijdig of volledig beschikbaar zijn van informatie?						
I8	**Overige risico's** Signaleert u nog andere risico's als gevolg van het niet juist, volledig of tijdig beschikbaar zijn van informatie? En wat zijn hiervan de mogelijke effecten?						
IT	**Totaal** Samenvattend, rekening houdend met de notering hierboven, wat is in het ergste geval het effect op de bedrijfsvoering of de patiëntenzorg wanneer de informatie uit de applicatie niet juist, volledig of tijdig beschikbaar is?						

Formulier 3: Vertrouwelijkheid (exclusiviteit)

Mogelijke effecten van onthulling van vertrouwelijke of gevoelige (financiële) informatie aan ongeautoriseerden.		**Classificatie** 5 Continuïteitsbedreiging 4 Serieuze schade 3 Behoorlijke schade 2 Minimaal effect 1 Te verwaarlozen					**Toelichting**
V1	**Directe schade voor de bedrijfsvoering of patiëntenzorg.** Hoe ernstig zijn de directe gevolgen voor de bedrijfsvoering of voor de patiëntenzorg wanneer vertrouwelijke of gevoelige (financiële) informatie onthuld wordt aan ongeautoriseerden?						
V2	**Verlies van vertrouwen** Wat is het mogelijke effect op het vertrouwen van patiënten of de reputatie van de organisatie wanneer vertrouwelijke of gevoelige (financiële) informatie onthuld wordt aan ongeautoriseerden?						
V3	**Wet- en regelgeving** Wat is het effect van het mogelijk niet (kunnen) naleven van wet- en regelgeving als gevolg van het onthullen van vertrouwelijke of gevoelige (financiële) informatie aan ongeautoriseerden?						
V4	**Additionele kosten** Wat is het mogelijke effect van additionele kosten die kunnen ontstaan als gevolg van het onthullen van vertrouwelijke of gevoelige (financiële) informatie aan ongeautoriseerden?						
V5	**Moraal van de medewerkers** Wat is mogelijk het effect op de moraal van de medewerkers wanneer vertrouwelijke of gevoelige (financiële) informatie wordt onthuld aan ongeautoriseerden.						
V6	**Fraude** Het beschikken over vertrouwelijke of gevoelige (financiële) informatie zou kunnen leiden tot fraude. Wat is het mogelijke effect hiervan?						
V7	**Overige risico's** Signaleert u nog andere risico's/consequenties van onopzettelijk of ongeautoriseerde onthulling van vertrouwelijke of gevoelige (financiële) informatie aan ongeautoriseerden?						
VT	**Totaal** Samenvattend, rekening houdend met de notering hierboven, wat is in het ergste geval het effect op de bedrijfsvoering of de patiëntenzorg wanneer vertrouwelijke of gevoelige (financiële) informatie wordt onthuld aan ongeautoriseerden?						

Formulier 4: bedreigingen t.a.v. beschikbaarheid/continuïteit

Mogelijke bedreigingen		Kans 5 Hoogstwaarschijnlijk 4 Waarschijnlijk 3 Mogelijk 2 Onwaarschijnlijk 1 Niet mogelijk					Toelichting
BB1	***Grote rampen of calamiteiten*** *Denk hierbij aan schade als gevolg van specifieke rampen zoals brand, overstroming, extreme weercondities (zoals storm, blikseminslag), fysieke schade (zoals vernieling of sabotage door terroristen, patiënten of werknemers), uitval van omgevingsapparatuur (airco), uitval van het netwerk, uitval van nutsvoorzieningen of het niet beschikbaar zijn van werknemers (door staking, ziekteverzuim etc.).*						
BB2	***Onvoldoende maatregelen voor IT-continuïteit*** *Denk hierbij aan factoren als continuïteitsmaatregelen voor kritische componenten van het systeem (bv. gegevens, processors/servers, werkstations, communicatienetwerken, opslagunits, software); gedocumenteerde continuïteitsplanning, procedures en het testen hiervan.*						
BB3	***Onvoldoende bedrijfscontinuïteitsplannen*** *Denk hierbij aan factoren zoals de geschiktheid van continuïteitsplannen van de afdeling tijdens het uitvallen van systemen; maatregelen voor herstel van de oorspronkelijke situatie met daarop volgend het opstarten van de diensten; documentatie van plannen; en het testen van continuïteitsprocedures.*						
BB4	***Het uitvallen van systemen*** *Denk hierbij aan factoren die te maken hebben met de kwetsbaarheid ten aanzien van het slecht functioneren van applicaties en systeemsoftware, hardware en communicatieapparatuur waaronder de stabiliteit van de systemen, de onderhoudbaarheid van de systemen, kwaliteit van acceptatietests, scheiding van productie- en testomgeving, etc.*						
BB5	***Degradatie van prestaties van het systeem*** *Denk hierbij aan de kwetsbaarheid ten aanzien van een onacceptabele degradatie van systemenprestaties, bv. voortkomend uit onvoldoende systeemcapaciteit om de normale werkdruk aan te kunnen; overbelast systeem tijdens pieken in de werkdruk; performanceproblemen in verband met 'wrijving' met andere applicaties op hetzelfde platform.*						
BB6	***Eventuele andere bedreigingen voor de beschikbaarheid van systemen/gegevens*** *Zijn er eventuele andere (externe of interne) bedreigingen die invloed kunnen hebben op de beschikbaarheid van systemen/gegevens? Denk hierbij aan factoren zoals verlies van primaire werknemers/beheerders; gegevensdiefstal, diefstal van software of apparatuur; verlies van gegevens tijdens een transmissie; computervirussen.*						
BBT	***Totaal*** *Gezien het bovenstaande: wat is de kans dat de applicatie (tijdelijk) niet beschikbaar is of informatie vanuit deze applicatie niet benaderbaar is?*						

Formulier 5: bedreigingen t.a.v. integriteit

Mogelijke bedreigingen		Kans 5 Hoogstwaarschijnlijk 4 Waarschijnlijk 3 Mogelijk 2 Onwaarschijnlijk 1 Niet mogelijk					Toelichting
BI1	***Invoer- en gebruikersfouten*** *Denk hierbij aan factoren als de kwaliteit van gebruikers (opleiding/training) en gebruikershandleidingen; controle op de invoer van gegevens; procedures voor het onderzoeken en corrigeren van invoerfouten; het loggen van activiteiten van gebruikers; controles op volledigheid en accuratesse van de invoer; beoordelingen van resultaten die geproduceerd zijn door het systeem.*						
BI2	***Programmafouten*** *Denk hierbij aan factoren als de kwaliteit van systeemdocumentatie; leeftijd, betrouwbaarheid en onderhoudbaarheid van software; frequentie en complexiteit van wijzigingsaanvragen; kwaliteit van de procedure voor wijzigingscontroles (inclusief programma versie controle, het testen van systemen en programma's, afspraken over gebruikersacceptatietesten).*						
BI3	***Ongeautoriseerd gebruik en toegang*** *Denk hierbij aan factoren als controles op fysieke en logische toegang tot systemen; gebruik van unieke user-ID onder de werknemers; geheimhouding van wachtwoorden; procedures voor het rapporteren en onderzoeken van pogingen tot beveiligingsovertredingen; toegang tot systemen door derden; logging.*						
BI4	***Operating fouten*** *Denk hierbij aan factoren als de kwaliteit van de bedieningsinstructies voor beheerders; instructies voor back-up en restore; bedieningsfouten bij het dagelijks beheer van systemen.*						
BI5	***Onvoldoende integriteit beheerders*** *Denk hierbij aan factoren als de controle op aanname van beheerders; controle op logische toegangbeveiliging beheerders; supervisie over beheerders; het loggen van de activiteiten van de beheerders.*						
BI6	***Integriteitsproblemen met aanleverende systemen*** *Denk hierbij aan factoren als de integriteit van en het soort aanvoersysteem; het soort gegevens dat deze systemen aanlevert; de beveiliging van aanleverende systemen; en de kwaliteit van controles op gegevensinvoer en goedkeuring van het aanleverende systeem.*						
BI7	***Andere bedreigingen omtrent de integriteit van systemen/gegevens.*** *Zijn er eventuele andere (externe of interne) bedreigingen die invloed kunnen hebben op de integriteit van systemen/gegevens.* *Denk hierbij ook aan de volledigheid van de totale controles om het verlies van integriteit van systemen en gegevens te voorkomen, te bespeuren en te herstellen.*						
BIT	***Totaal*** *Gezien het bovenstaande: wat is de kans dat de integriteit van informatie op enigerlei wijze wordt geschaad?*						

Formulier 6: bedreigingen t.a.v. vertrouwelijkheid

Mogelijke bedreigingen		Kans 5 Hoogstwaarschijnlijk 4 Waarschijnlijk 3 Mogelijk 2 Onwaarschijnlijk 1 Niet mogelijk					Toelichting
BV1	***Derden krijgen inzicht in geprinte informatie of documentatie*** *Denk hierbij aan factoren als in hoeverre gevoelige informatie verspreid wordt via documenten of prints; het gebruik van prints of documenten buiten het bedrijf (bv. omdat medewerkers thuis werken); de opslag van prints en documenten; het bewustzijn onder werknemers en management van het belang van vertrouwelijkheid; het bestaan van een cleandesk-beleid.*						
BV2	***Ongeautoriseerde toegang tot de organisatie*** *Denk hierbij aan factoren als beperking van de toegang tot het gebouw; kwaliteit van het beveiligingspersoneel; het delen van gebouwen; uitdiensttredingsprocedure, gebruik van extern gecontracteerd personeel (bv. schoonmakers); opslag van documenten en prints in het gebouw; het gebruik van een geheimhoudingsverklaring voor ingehuurd personeel.*						
BV3	***Ongeautoriseerde toegang tot gegevens door werknemers*** *Denk hierbij aan factoren als de kwaliteit van logische/fysieke toegangsbeveiliging tot applicatiegegevens; gebruik van unieke user-ID door werknemers; geheimhouding van wachtwoorden onder werknemers; procedures voor het verwijderen van toegangsrechten als een werknemer van functie verandert of de organisatie verlaat; het loggen van toegangspogingen; procedures voor het rapporteren en onderzoeken van mogelijke beveiligingsovertredingen.*						
BV4	***Ongeautoriseerde toegang tot gegevens door extern personeel*** *Denk hierbij aan factoren als de kwaliteit van controles omtrent fysieke/logische toegang tot applicatiegegevens; controle over inbeltoegang; beperkingen in het gebruik van het internet; gebruik van firewalls; gebruik van laptops; toegang tot systemen door derden; loggen van toegangspogingen.*						
BV5	***Onderschepping van communicatieverbindingen*** *Denk hierbij aan factoren als de frequentie van het versturen van gevoelige informatie; schaal en complexiteit van het netwerk; fysieke beveiliging van interne communicatielijnen en benodigde apparatuur; soorten externe communicatie (bv huurlijn, internet, etc); gebruik van encryptie; netwerkmanagement procedures.*						
BV6	***Andere bedreigingen voor de vertrouwelijkheid van systemen/gegevens.*** *Zijn er eventuele andere (externe of interne) bedreigingen die de applicatie kwetsbaar maken en kunnen de vertrouwelijkheid schaden?*						
BVT	***Totaal*** *Gezien het bovenstaande: wat is de kans dat de vertrouwelijkheid van informatie op enigerlei wijze wordt geschaad?*						