TASKFORCE
Bestuur & Informatieveiligheid Dienstverlening

Risicoanalysemethode

Een operationeel product op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR)

Rijksoverheid VNG Vereniging van Nederlandse Gemeenten Interprovinciaal Overleg ip MANIFESTgroep UNIE VAN WATERSCHAPPEN

Colofon

Onderhavig operationeel product, behorende bij de Baseline Informatiebeveiliging Rijksdienst (BIR), is mogelijk gemaakt door de Taskforce Bestuur en Informatieveiligheid Dienstverlening (Taskforce BID). Het product is gebaseerd op het operationele product ‘Diepgaande Risicoanalysemethode gemeenten’ behorende bij de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit product is ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (IBD).

Leeswijzer

Dit document is een van de operationele producten op basis van de Baseline Informatiebeveiliging Rijksdienst (BIR).

Doel

Dit document biedt een methodische aanpak om een risicoanalyse uit te voeren, indien dit op basis van het uitvoeren van de Quickscan BIR noodzakelijk is gebleken.

Doelgroep

Dit document is van belang voor het verantwoordelijke management, de systeemeigenaren, proceseigenaren, applicatiebeheerders en de ICT-organisatie van een organisatie binnen de Rijksoverheid.

Reikwijdte

Dit document heeft voornamelijk betrekking op de maatregelen 10.8.5.1 en 15.1.4.1 van de Baseline Informatiebeveiliging Rijksdienst (BIR). Het document gaat in op personele, organisatorische en technische informatiebeveiligingsaspecten die organisaties binnen de Rijksoverheid dienen te overwegen om te bepalen of de baseline voldoende beveiliging biedt.

Relatie met overige producten

- Baseline Informatiebeveiliging Rijksdienst (BIR). Tactisch Normenkader (TNK)
- Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)
- Informatiebeveiligingsbeleid
- Quickscan BIR

Inhoudsopgave

1 Inleiding 5

1.1 Aanpak 5

1.2 Uitvoering 5

1.3 Planning 6

2 Informatiesysteem in kaart brengen 7

3 Analyse van dreigingen 8

4 Bepalen maatregelen 9

Bijlage A. Model om informatiesysteem in kaart te brengen 10

Bijlage B. Model om dreigingen in kaart te brengen 15

Bijlage C. Tabel voor bepalen effect dreigingen 23

Bijlage D: Dreigingen specifiek voor soorten informatiesystemen 24

Bijlage E: Model voor overzicht maatregeldoelstellingen 26

Bijlage F: Model voor detailoverzicht maatregeldoelstellingen 29

Bijlage G: Risico's en bedreigingen 31

1 Inleiding

De Baseline Informatiebeveiliging Rijksdienst (BIR) is de basis voor informatiebeveiligingsmaatregelen voor organisaties binnen de Rijksoverheid. Voor het merendeel van de systemen voor de processen is het basisbeschermingsniveau van de BIR voldoende. Er kunnen zich situaties voordoen waarbij er meer maatregelen nodig zijn. Om dit te onderzoeken is de Quickscan BIR ontwikkeld. Het is verstandig om de Quickscan uit te voeren om vast te stellen of het BIR-beschermingsniveau voor bepaalde processen of systemen voldoende is. Ook bij wijzigingen van systemen of de initiatie van een nieuw project zijn goede aanleidingen voor het uitvoeren van de Quickscan en eventueel een daaropvolgende risicoanalyse.

Als uit de Quickscan BIR volgt dat de wijziging van het systeem of het project binnen de beveiligingsnormen van de BIR valt, kan worden volstaan met de Baseline Informatiebeveiliging Rijksdienst. Wanneer de beschikbaarheids-, integriteits- en vertrouwelijkheidseisen van een proces of systeem boven de beveiligingsnormen van de BIR uitkomen, moet een diepgaandere risicoanalyse worden uitgevoerd. Dit document beschrijft de wijze waarop een risicoanalyse wordt uitgevoerd en de tools die daarbij gebruikt worden.

De doelstelling van de risicoanalyse is om in kaart te brengen welke maatregelen aanvullend op de baseline moeten worden getroffen om het juiste niveau van beveiliging te realiseren voor een bepaald proces of systeem.

1.1 Aanpak

Deze diepgaande risicoanalyse behelst tevens een quick scan aanpak die er voor zorgt dat op een pragmatische en effectieve manier de juiste zaken in kaart worden gebracht. In de Quickscan BIR ligt de nadruk op het proces dat afhankelijk is van informatievoorziening. In deze risicoanalyse ligt de nadruk op de informatievoorziening die het proces ondersteunt. De maatregelen die worden opgeleverd, omvatten wel het volledige scala van organisatie tot technologie. Het uitgangspunt van de risicoanalyse is dat de Quickscan BIR al is uitgevoerd en dat de resultaten daarvan beschikbaar zijn. De risicoanalyse wordt uitgevoerd na de Quickscan als de uitkomst hiertoe aanleiding geeft.

1.2 Uitvoering

De risicoanalyse bestaat uit 3 hoofdstappen:

1. Het in kaart brengen van de onderdelen van de informatievoorziening conform het MAPGOOD model[1].
2. Het in kaart brengen van de dreigingen die relevant zijn voor het te onderzoeken informatiesysteem, met per dreiging het potentiële effect en de kans op optreden.
3. Het vertalen van de meest relevante dreigingen naar maatregelen die moeten worden getroffen.

Bij stap 2 mag geen rekening gehouden worden met reeds bestaande maatregelen die dreigingen verminderen. Dit beïnvloedt de uitslag van de risicoanalyse. De risicoanalyse dient zo ongekleurd en neutraal als mogelijk te worden ingevuld, alsof er nog geen maatregelen bestaan.

[1] Zie hoofdstuk twee en bijlage A.

Het uitvoeren van een risicoanalyse dient te worden ondersteund door een medewerker met ervaring bij het uitvoeren van risicoanalyses. Het is aan te bevelen dat de organisatie een medewerker aanstelt die de risicoanalyse uitvoert en op deze manier ervaring met het uitvoeren van risicoanalyses opbouwt. Dit zal de kwaliteit van het uitvoeren van volgende risicoanalyses verhogen. Tijdens de risicoanalyse ligt de nadruk op procesbewaking en kwaliteitsbewaking door het stellen van het stellen van controlevragen om de verschillende inschattingen tussen de deelnemers van de risicoanalyse te toetsen.

1.3 Planning

De drie stappen die hierboven genoemd zijn, hebben ongeveer het volgende tijdsbeslag:

	Stap 1 Informatiesysteem in kaart brengen	**Stap 2 Analyse dreigingen**	**Stap 3 Bepalen maatregeldoelstellingen**
Voorbereiding	Analist 4 uur Systeemeigenaar 20 minuten	Analist 6 uur	Analist 10 tot 12 uur
Interview/sessie	Analist 4 uur Systeemeigenaar 4 uur (eventueel technisch en functioneel beheer erbij)	Analist 4 uur Systeemeigenaar 4 uur	Analist 2 uur Systeemeigenaar 2 uur
Uitwerking	Analist 4 uur	Analist 8 uur	Analist 14 uur

2 Informatiesysteem in kaart brengen

Inzicht in de informatievoorziening is nodig om in de volgende stap de bedreigingen goed in kaart te kunnen brengen. Hiervoor wordt het MAPGOOD-model toegepast om alle componenten van de informatievoorziening in kaart te brengen. MAPGOOD staat voor: Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving en Diensten.

In bijlage A is een template hiervoor opgenomen. Het template moet volledig worden ingevuld door de systeemeigenaar, eventueel met hulp van de functioneel beheerder en/of een technisch beheerder. De systeemeigenaar kan ook de proceseigenaar betrekken in dit proces.

Belangrijk is dat ieder MAPGOOD-component volledig in kaart wordt gebracht, zodat alle relevante onderdelen van de informatievoorziening bekend zijn. De volledigheid op hoofdcomponent niveau is belangrijk om later bedreigingen en maatregelen goed te kunnen toewijzen. Daarnaast is het belangrijk dat goed onderscheid wordt gemaakt tussen de zaken waar de systeemeigenaar direct voor verantwoordelijk is en de zaken die zijn uitbesteed aan een externe partij en daarom onder het component ‘Dienst’ vallen.

De volgende werkwijze wordt gehanteerd:

- De systeemeigenaar en een analist en/of de CISO bespreken in 30 minuten de bedoeling van het MAPGOOD-overzicht. Gebruik eventueel systeemdocumentatie als deze voorhanden is.
- De systeemeigenaar (eventueel geholpen door functioneel en technisch beheer) vult het overzicht in. Hier zijn naar verwachting maximaal 4 uren voor nodig.
- De systeemeigenaar en analist en/of de CISO bespreken in 30 tot 60 minuten de invulling.

Een alternatieve methode kan zijn dat de partijen in een gezamenlijke sessie/workshop (max. 2 uur) de MAPGOOD-componenten in kaart brengen. Hiervoor zijn op zijn minst de analist en de systeemeigenaar nodig.

3 Analyse van dreigingen

Op basis van een standaard invullijst met dreigingen (zie bijlage B) worden door de analist samen met de systeemeigenaar de relevante bedreigingen in kaart gebracht. Het betreft hier bedreigingen waardoor een verlies aan beschikbaarheid, integriteit of vertrouwelijkheid van de informatievoorziening kan ontstaan. In deze sessie wordt per MAPGOOD-component besproken wat het effect is van het ‘onjuist werken’, ‘(tijdelijk) niet werken’ of ‘niet aanwezig zijn’ van deze component. Zoals eerder beschreven, mag hierbij geen rekening gehouden worden met reeds bestaande maatregelen die dreigingen verminderen.

De dreigingen worden in de vorm van incidenten verwoord en per incident wordt op een 3-puntsschaal (Laag ‘L’; Midden ‘M’; Hoog ‘H’) aangegeven hoe groot de invloed ervan is op de werking van het informatiesysteem (de schade) en wat de kans is op het optreden van de betreffende dreiging. Op basis van een standaard tabel wordt bepaald wat het totale effect is (kans x schade). De tabel die hiervoor wordt gebruikt, is opgenomen in bijlage C.

De volgende werkwijze wordt gehanteerd:

- De analist bereidt de bespreking voor door:

  1. Uit de standaardlijst (bijlage B) de dreigingen te schrappen die zeker niet relevant zijn voor het informatiesysteem, en;
  2. Uit de applicatiespecifieke lijst (bijlage D) de dreigingen toe te voegen die mogelijk relevant zijn voor het informatiesysteem. Inspanning is circa 2 uur.

- De analist en systeemeigenaar (eventueel met functioneel beheerder) vullen het bijgestelde model van dreigingen in. Daarbij geven zij voor iedere dreiging aan wat de kans van optreden is, wat de mogelijke schade is en geven hier een toelichting op. De doorlooptijd van deze activiteit is naar schatting 4 uur. Bij een complex systeem kan 8 uur worden gerekend.

- De analist werkt de invulling uit waarbij zorg gedragen wordt voor de bepaling van de kans x schade en een uitwerking van de toelichtingen. Op basis van de berekening van de kans x schade wordt bepaald welke dreigingen het meest relevant worden geacht. De inspanning is circa 4 tot 8 uur.

4 Bepalen maatregelen

In deze stap worden de maatregelen bepaald die moeten worden getroffen om de dreigingen het hoofd te bieden, die in de vorige stap als meest belangrijk zijn benoemd. De maatregelen worden daarbij geformuleerd op het niveau van doelstellingen (controls) om ervoor te zorgen dat bij de invulling rekening kan worden gehouden met de stand van zaken op dat moment. Tevens kan hiermee een leverancier functioneel worden aangestuurd in plaats van op het niveau van detailmaatregelen.

De volgende werkwijze wordt gehanteerd:

- De analist controleert of de dreigingen die niet ‘H’ of ‘HH’ (zie ook bijlage C) zijn geclassificeerd inderdaad door de BIR worden afgedekt. Inspanning is 1 á 2 uur.
- De analist vertaalt de dreigingen naar maatregeldoelstellingen die moeten worden getroffen. Op basis van de BIR en kennis van het onderhavige proces en informatiesysteem wordt het overzicht voor maatregeldoelstellingen in ingevuld (bijlage E). Hierin zijn alle gegevens in één overzicht bij elkaar gebracht. Als het goed is, zijn alleen bepaalde vakken ingevuld. Inspanning is 4 á 8 uur.
- De analist en de systeemeigenaar bespreken het overzicht om zeker te stellen dat de juiste vertaling van dreigingen naar maatregeldoelstellingen is gemaakt en voegen eventuele additionele zaken toe. Doorlooptijd is 2 uur.
- De analist vertaalt het overzicht maatregeldoelstellingen naar het detailoverzicht (bijlage F). Daarbij wordt per maatregeldoelstellingen relevante toelichtingen en voorbeeldmaatregelen toegevoegd. Inspanning is circa 4 uur.

De analyse is hiermee afgerond. Het detailoverzicht met maatregeldoelstellingen wordt door systeemeigenaar en de coördinator IB of de CISO besproken om vast te stellen op welke manier de invoering van de maatregelen wordt georganiseerd. Daarbij kan ook worden gekozen om alternatieve maatregelen te implementeren, bepaalde risico’s te accepteren (beargumenteerd volgens het uitgangspunt ‘comply or explain’ en na een zorgvuldige kosten/baten-analyse ten aanzien van de benodigde maatregelen) of maatregelen op centraal niveau in plaats van op het niveau van het informatiesysteem te nemen. Hiervoor kan bijlage G worden gebruikt.

Bijlage A. Model om informatiesysteem in kaart te brengen

Componenten

De inventarisatie van de componenten van een informatiesysteem wordt uitgevoerd aan de hand van de zogenaamde MAPGOOD-componenten, MAPGOOD staat voor:

- **M**ens. De mensen die nodig zijn om het informatiesysteem te beheren en gebruiken;
- **A**pparatuur. De apparatuur die nodig is om het informatiesysteem te laten functioneren;
- **P**rogrammatuur. De programmatuur waaruit het informatiesysteem bestaat;
- **G**egevens. De gegevens die door het systeem worden verwerkt;
- **O**rganisatie. De organisatie die nodig is om het informatiesysteem te laten functioneren;
- **O**mgeving. De omgeving waarbinnen het informatiesysteem functioneert;
- **D**iensten. De externe diensten die nodig zijn om het systeem te laten functioneren.

Het is de bedoeling dat deskundigen - bijvoorbeeld de functioneel beheerder en technisch beheerder - de voornoemde componenten voor het eigen informatiesysteem beschrijven.

Invulling

Voor een specifiek informatiesysteem moeten de MAPGOOD-componenten in kaart worden gebracht. Het gaat om het invullen van de twee rechterkolommen in de hierna opgenomen tabel. Voeg waar nodig nieuwe rijen in. Bij het invullen moeten zowel de centrale, als de decentrale onderdelen worden meegenomen. Decentraal betreft bijvoorbeeld gebruikers van een bepaalde locatie, de PC en de infrastructuur die deze gebruiker nodig heeft, de gegevens en programmatuur die ter plaatse nodig zijn of het lokale beheer.

Aan het einde van deze bijlage A is een ingevuld voorbeeld opgenomen dat als hulp kan dienen voor het invullen van de MAPGOOD-componenten.

INVULLING MAPGOOD TEN BEHOEVE VAN INFORMATIESYSTEEM ...

Voor uitleg wordt verwezen naar hoofdstuk 2 en het bovenstaande. De onderstaande tabel dient te worden ingevuld op basis van MAPGOOD om vast te stellen uit welke componenten het informatiesysteem bestaat.

Component	**Onderdelen**	**Invulling**
Mens *(Welke mensen gebruiken het systeem?)*		
Apparatuur *(Welke apparatuur kent het systeem?)*		
Programmatuur *(Welke programmatuur kent het systeem?)*		
Gegevens *(Welke gegevens kent het systeem?)* **Let op:** persoonsgegevens apart benoemen!		
Organisatie *(Welke organisatieonderdelen hebben met het systeem te maken?)*		
Omgeving *(Welke fysieke omgevingen zijn er voor het systeem?)*		
Diensten *(Welke diensten*		

horen bij het systeem?)		

VOORBEELD: MAPGOOD tabel (beantwoording is willekeurig)

Component	**Onderdelen**	**Invulling**
Mens *(Welke mensen gebruiken het systeem?)*	Directe gebruikers	*Zorgbegeleider ...* *Medewerkers Zorgregistratie ...* *Medewerkers ...*
	Indirecte gebruikers	*Gebruikers afdeling ...* *Gebruikers front office organisatie ...* *Gebruikers afnemer ...*
	Functioneel applicatiebeheerder	*Functioneel beheerders afdeling <naam>*
	3e lijns applicatie support	*Is uitbesteed bij …*
	Technisch applicatiebeheer	*Is uitbesteed bij ...*
	Systeembeheer	*Is uitbesteed bij ...*
Apparatuur *(Welke apparatuur kent het systeem?)*	webserver/presentatie server applicatie server	*Server ... in serverruimte ...*
	database server	*Server ... in serverruimte ...*
	... ... server	*Server staat bij / op /in*
	Lokale PC voor script	*Computer van <naam>*
	Werkplekken van gebruikers	*Intern de standaard ... werkplekken* *Extern eigen werkplekken* *Heb ook aandacht waar deze werkplekken staan of wordt er op afstand gewerkt*
	Beheer werkplekken	*Beheerwerkplekken staan bij ... ten behoeve van …*

Programmatuur *(Welke programmatuur kent het systeem?)*	Microsoft besturingssysteem (.NET)	Software op presentatie server
	Internet Information Server (IIS) van Microsoft	Software op presentatie server
	Oracle Database v 9 (versie aanpassen)	*Software op database server*
	Microsoft Reporting Services	*Software op presentatie server*
	Maatwerkbeveiligingscomponenten (SSS)	*Software op server ...*
Gegevens *(Welke gegevens kent het systeem?)* **Let op:** persoonsgegevens apart benoemen	Zorgexploitatie gegevens Rapporten Financiële verantwoording	*Gegevens van mogelijke kosten en opbrengsten van (toekomstige) ...*
	Object gegevens	*...*
	Klantgegevens	*…*
	Autorisatiegegevens	*Gegevens betreffende de autorisatie die medewerkers hebben om met de applicatie te mogen werken.*
	Persoonsgegevens	*Het systeem maakt gebruik van de volgende persoonsgegevens:* *Medewerkers voor autorisatie / authenticatie binnen de applicatie* *Burgers: zaak gerelateerde informatie* *Wel/geen bijzondere persoonsgegevens* *Zo ja, welke bijzondere persoonsgegevens:* *Verwijs naar een eventuele uitgevoerde of uit te voeren PIA*
	Log gegevens	*Gegevens die het informatiesysteem opslaat met betrekking tot de transacties die worden uitgevoerd.(en wat bevatten die loggings)*

Organisatie *(Welke organisatieonderdelen hebben met het systeem te maken?)*	Beheerorganisatie	*De organisatie rond de functioneel beheerders*
	Gebruikersorganisatie	*De organisatie rond de gebruikers*
Omgeving *(Welke fysieke omgevingen zijn voor het systeem?)*	Adres	*Adres / locatie / bijzonderheden*
	Serverruimte	*Hier staan de centrale servers*
	Werkplekken ...	*Hier zitten de gebruiker en functioneel beheerders en staan de PC's en printers.*
	Beheerders	*..*
	Technisch applicatiebeheer	*Door dienstverlener*
Diensten *(Welke diensten horen bij het systeem?)*	Technisch systeembeheer (besturingssystemen, databases et cetera.)	*Uitgevoerd door ...*
	Netwerkinfrastructuur, netwerkdiensten (Inloggen, SSC, …), werkplekken, printers et cetera.	*Uitgevoerd door ...*
	Onderhoudscontract en strippenkaart	*Bij ...*

Bijlage B. Model om dreigingen in kaart te brengen

Door de analist wordt samen met de systeemeigenaar de relevante bedreigingen in kaart gebracht. Het betreft bedreigingen waardoor verlies aan beschikbaarheid, integriteit of vertrouwelijkheid van de informatievoorziening kan ontstaan. In deze sessie wordt per MAPGOOD-component (bijvoorbeeld Mens) besproken wat het effect is van het ‘onjuist werken’, ‘(tijdelijk) niet werken’ of ‘niet aanwezig zijn’ van deze component. Let hierbij wel op dat geen rekening mag worden gehouden met al bestaande maatregelen die dreigingen verminderen.

De dreigingen worden in de vorm van incidenten verwoord en per incident wordt op een 3-puntsschaal (Laag ‘L’; Midden ‘M’; Hoog ‘H’) aangegeven hoe groot de invloed ervan is op de werking van het informatiesysteem (de schade), en wat de kans is op het optreden van de betreffende dreiging. Op basis van een standaard tabel wordt bepaald wat het totale effect is (kans x schade). Zie ook bijlage D voor specifieke dreigingen die kunnen worden toegevoegd.

Er kunnen binnen de organisatie ook al eerder dreiging- en risicoanalyses zijn uitgevoerd, eventuele dreigingen die hier al vastgesteld zijn, kunnen ook worden meegenomen.

Component	**Incident**	**Schade (L,M,H)**	**Kans (L,M,H)**	**Totaal (L,M,H)**	**Toelichting (gevolgen et cetera)**
Mens • Functioneert onjuist • Niet aanwezig • Niet in dienst	Wegvallen: • Voorzienbaar (ontslag, vakantie) • Onvoorzienbaar (ziekten, overlijden, ongeval, staking)				
	Onopzettelijk foutief handelen: • Onkunde, slordigheid • Foutieve procedures • Complexe foutgevoelige bediening • Onzorgvuldige omgang met wachtwoorden • Onvoldoende kennis/training				
	Opzettelijk foutief handelen:				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
	• Niet werken volgens voorschriften/procedures • Fraude/diefstal/lekken van informatie • Ongeautoriseerde toegang met account van medewerker met hogere autorisaties				
Apparatuur • Functioneert onjuist • Stoort • Gaat verloren of raakt ernstig beschadigd	Spontaan technisch falen: • Veroudering/slijtage • Storing • Ontwerp/fabricage/installatie/onderhoudsfouten				
	Technisch falen door externe invloeden: • Stroomuitval • Slechte klimaatbeheersing • Nalatig onderhoud door schoonmaak • Natuurgeweld • Diefstal/schade				
	Menselijk handelen/falen: • Installatiefout • Verkeerde instellingen • Bedieningsfouten • Opzettelijke aanpassingen/sabotage • Beschadiging/vernieling • Verlies/diefstal (onder andere. verlies USB-sticks of andere				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
	gegevensdragers) • Verwijdering van onderdelen waardoor storingen ontstaan				
Programmatuur • Functioneert onjuist • Loopt vast of vertraagde uitvoering • Gaat verloren of raakt ernstig beschadigd	Nalatig menselijk handelen: • Ontwerp-, programmeer-, invoering, beheer/onderhoudsfouten • Introductie van virus en dergelijke. door gebruik van niet gescreende programma's • Gebruik van de verkeerde versie van programmatuur • Slechte documentatie				
	Onopzettelijk menselijk handelen: • Fouten door niet juist volgen van procedures • Installatie van malware en virussen door gebruik van onjuiste autorisaties				
	Opzettelijk menselijk handelen: • Manipulatie voor of na ingebruikname • (Ongeautoriseerde) functieverandering en/of toevoeging • Installatie van virussen, Trojaanse paarden en dergelijke • Kapen van autorisaties van collega's • Illegaal kopiëren van programmatuur • Oneigenlijk gebruik of privégebruik van bedrijfsprogrammatuur				
	Technische fouten/mankementen: • Fouten in code programmatuur die de werking verstoren				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
	• Achterdeuren in programmatuur voor (onbevoegde) toegang • Bugs/fouten in code die tot exploits kunnen leiden				
	Organisatorische fouten: • Leverancier gaat failliet • Geen goede afspraken met leverancier				
Gegevens • Worden onterecht ontsloten • Zijn tijdelijk ontoegankelijk • Gaan verloren	Via gegevensdragers (CD/DVD/USB-sticks/Harddisk/Back-ups/mobiele apparaten): • Diefstal/zoekraken/lekken • Beschadiging door verkeerde behandeling • Niet overeenkomende bestandformaten • Foutieve of geen versleuteling • Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen				Privacy inbreuk burgers benoemen
	Via Cloud voorzieningen: • Ongeautoriseerde toegang door onbevoegden (hackers/hosters) • Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)				
	Via apparatuur: • Fysieke schrijf- of leesfouten • Onvoldoende toegangsbeperking tot apparatuur • Fouten in interne geheugens				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
	• Aftappen van gegevens				
	Via programmatuur: • Foutieve of gemanipuleerde programmatuur • Doorwerking van virussen/malware • Afbreken van verwerking				
	Via personen: • (On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data • Onbevoegde toegang door onbevoegden • Onbevoegd kopiëren van gegevens • Meekijken over de schouder door onbevoegden • Onzorgvuldige vernietiging • Niet toepassen clear screen/clear desk • Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties) • Oneigenlijk gebruik van autorisaties • Toegang verschaffen tot gegevens door middel van identiteitsfraude of social engineering				
Organisatie • Werkt niet volgens vastgestelde uitgangspunten	Gebruikersorganisatie: • Mismanagement • Gebrekkige toedeling taken, bevoegdheden, verantwoordelijkheden				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
• Reorganiseert • Fuseert of wordt opgeheven	• Onduidelijke of ontbrekende gedragscodes • Afwezige, verouderde of onduidelijke handboeken /systeemdocumentatie / werkprocedures/ gebruiksinstructies • Onvoldoende interne controle • Onvoldoende toetsing op richtlijnen • Onvoldoende of geen contractbeheer • Ontbrekende of onduidelijke SLA's • Gebrekkige doel/middelen beheersing				
	Beheerorganisatie: • Gebrekkig beleid betreffende beheer • Onvoldoende kennis of capaciteit • Onvoldoende kwaliteitsborging • Onvoldoende beheer van systemen en middelen				
	Ontwikkelingsorganisatie: • Slecht projectmanagement • Niet volgen van projectenkalender of PPM • Geen ontwikkelrichtlijnen en/of – procedures • Er worden geen methoden/technieken gebruikt • Gebrek aan planmatig werken				
Omgeving • Is toegankelijk voor	Huisvesting: • Ongeautoriseerde toegang tot gebouw(en)				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
ongeautoriseerden • Is beschadigd • Is verwoest of ernstig beschadigd	• 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				
	Nutsvoorzieningen: • Uitval van elektriciteit, water, telefoon • Wateroverlast door lekkage, bluswater • Uitval van licht-, klimaat- en,sprinklerinstallatie				
	Buitengebeuren: • Natuurgeweld (overstroming, blikseminslag, storm, aardbeving et cetera) • Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig) • Blokkade/staking • Onveilige, geblokkeerde, vluchtwegen bij brand				
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				

Component	Incident	Schade (L,M,H)	Kans (L,M,H)	Totaal (L,M,H)	Toelichting (gevolgen et cetera)
	getekende geheimhoudingsverklaringen • Voert wanbeheer, slordigheden in beheersactiviteiten, • Werkt niet conform ITIL of BiSL principes • Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie • Houdt zich niet aan functiescheiding • Maakt gebruik van te zware autorisatie, niet functie gebonden				
	Diensten dienstverlener tijdelijk niet beschikbaar: • Levert diensten niet conform overeenkomst • Onderbreking dienstverlening door overname dienstverlener • Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen en dergelijke) • Past verkeerde prioriteiten toe in klantbejegening • Levert onvoldoende capaciteit voor een goede dienstverlening				
	Diensten dienstverlener definitief niet meer te leveren: • Een dienstverlener gaat failliet • Opzegging diensten door dienstverlener				

Bijlage C. Tabel voor bepalen effect dreigingen

Deze tabel wordt gebruikt om de ernst van de bedreigingen vast te stellen. Deze wordt ingevuld in de kolom ‘totaal’ van de tabel in de voorgaande bijlage. Wanneer een bedreiging bijvoorbeeld een kans ‘midden’ heeft en de potentiële schade ‘hoog’ is, dan wordt uit de tabel afgeleid dat de totale uitkomst op ‘hoog’ uitkomt voor die specifieke dreiging.

		SCHADE		
		H	**M**	**L**
KANS	**H**	HH	H	M
	M	H	M	L
	L	M	L	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 eerder vastgestelde dreigingen die expliciet relevant zijn voor het onderhavige informatiesysteem. Deze bijlage beschrijft een aantal soorten informatiesystemen met de bijbehorende specifieke dreigingen.

De vooringevulde lijst met dreigingen bevat alleen de algemene dreigingen. Uit onderstaande lijst worden potentiële dreigingen toegevoegd (zie hoofdstuk 3, stap 1, punt 2 voor 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 bijbehorende specifieke dreigingen verder worden aangevuld.

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 organisatie
- 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.

Bijlage E: Model voor overzicht maatregeldoelstellingen

Onderstaand schema dient als een middel om globaal en snel inzicht te krijgen. De resultaten van de voorgaande stappen worden ingevuld, inclusief het resultaat van de Quickscan. Hier worden alleen die bedreigingen en bijbehorende maatregeldoelstellingen opgenomen die bedreigingen wegnemen of tegengaan boven een bepaald niveau, bijvoorbeeld alle dreigingen die een waardering hebben van ‘HH’ of “H’. Op basis van ervaring weten we dat dit veel toegevoegde waarde heeft.

De analist vult in op basis van de besproken bedreigingen en bespreekt met de systeemeigenaar om te verifiëren dat op de juiste punten de focus wordt gelegd.

			BESCHIKBAARHEID opnemen eis en kleur in hoogte eis zetten	CONTINUÏTEIT opnemen eis en kleur in hoogte eis zetten	INTEGRITEIT opnemen eis en kleur in hoogte eis zetten	VERTROUWELIJKHEID opnemen eis en kleur in hoogte eis zetten	PRIVACY opnemen eis en kleur in hoogte eis zetten
			Opnemen motivatie voor de gestelde eis uit de baselinetoets.	Opnemen motivatie voor de gestelde eis uit de baselinetoets.	Opnemen motivatie voor de gestelde eis uit de baselinetoets.	Opnemen motivatie voor de gestelde eis uit de baselinetoets.	Opnemen motivatie voor de gestelde eis uit de baselinetoets.
MAPGOOD **IB-GEBIED**	**MENS**	**APPARATUUR**	**PROGRAMMATUUR**	**GEGEVENS**	**ORGANISATIE**	**OMGEVING**	**DIENSTEN**
	Opnemen beschrijving	Opnemen beschrijving	Opnemen beschrijving	Opnemen beschrijving	Opnemen beschrijving	Opnemen beschrijving MAPGOOD component	Opnemen beschrijving

	MAPGOOD component MENS	MAPGOOD component APPARATUUR	MAPGOOD component PROGRAMMATUUR	MAPGOOD component GEGEVENS	MAPGOOD component ORGANISATIE	OMGEVING	MAPGOOD component DIENSTEN
BIR hoofdstuk							
IB-beleid en -plan							
Organisatie van IB en externe partijen							
Classificatie en beheer van informatie en bedrijfsmiddelen							
Personele beveiligingseisen							
Fysieke beveiliging							
Beheer van communicatie- en bedieningsprocessen							
Logische toegangsbeveiliging							
Ontwikkeling en onderhoud van systemen							
Beheer van beveiligingsincidenten							

Continuïteit							
Naleving							

Bijlage F: Model voor detailoverzicht maatregeldoelstellingen

Onderstaand model is een detaillering van de voorgaande tabel. Hier moeten per BIR-onderwerp de maatregeldoelstellingen worden uitgewerkt door de analist. Het is aan te bevelen om de BIR GAP-analyse te gebruiken omdat daar al veel voorbeeld maatregelen staan. Als de BIR GAP-analyse al is uitgevoerd, is er inzicht in de beveiligingsmaatregelen die reeds zijn ingevoerd. De derde kolom kan voor toelichting en voorbeelden worden gebruikt. De laatste kolom wordt tenslotte ingevuld op basis van de risicoafweging en afspraken over de verantwoordelijkheid ten aanzien van de maatregel. De maatregelen kunnen het beste worden genummerd, zodat er later naar verwezen kan worden. Er kan ook verwezen worden naar een BIR maatregelnummer.

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	Invoeringswijze (in te vullen door organisatie)
IB-beleid en plan	MAATREGELDOELSTELLINGEN OVERNEMEN UIT OVERZICHT TABEL	OPNEMEN TOELICHTINGEN EN VOORBEELDMAATREGELEN	
Organisatie IB			
Classificatie en beheer van informatie en bedrijfsmiddelen			
Personele beveiligingseisen			
Fysieke beveiliging			
Beheer van communicatie- en bedieningsprocessen			

Informatie-beveiligingsgebied	Maatregeldoelstelling	Toelichting en voorbeeldenmaatregelen.	Invoeringswijze (in te vullen door organisatie)
Logische Toegangsbeveiliging			
Ontwikkeling en onderhoud van systemen			
Continuïteit			
Naleving			

Bijlage G: Risico's en bedreigingen

Deze bijlage is een hulpmiddel om over de dreigingen, de schade en kans en uitleg te geven of het risico geaccepteerd is door de systeemeigenaar, en als er maatregelen gekozen zijn welke dat dan zijn. Dit dient als input voor een systeembeveiligingsplan of informatiebeveiligingsplan. Aan deze tabel moeten de eerder zelf toegevoegde dreigingen nog worden toegevoegd.

Bedreigingen per groep		Kans			Schade			Geaccepteerd risico	Maatregel? + maatregel nummer, bestaande BIR maatregel + nummer
Mensen	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Wegvallen	Voorzienbaar (ontslag, vakantie)								
	Onvoorzienbaar (ziekten, overlijden, ongeval, staking)								
Onopzettelijke foutief handelen	Onkunde, slordigheid								
	Foutieve procedures								
	Complexe foutgevoelige bediening								
	Onzorgvuldige omgang met wachtwoorden								
	Onvoldoende kennis/training								
Opzettelijke foutief handelen	Niet werken volgens voorschriften/procedures								
	Fraude/diefstal/lekken van informatie								
	Ongeautoriseerde toegang met account van medewerker met hogere autorisaties								
Apparatuur	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Spontaan technisch falen	Veroudering/slijtage								

	Storing								
	Ontwerp/fabricage/installatie-onderhouds fouten								
Technisch falen door externe invloeden	Stroomuitval								
	Slechte klimaatbeheersing								
	Nalatig onderhoud door schoonmaak								
	Elektromagnetische straling								
	Elektrostatische lading								
	Diefstal/schade								
Menselijk handelen/falen	Bedieningsfouten								
	Opzettelijke aanpassingen/sabotage								
	Beschadiging/vernieling								
	Verlies/diefstal (onder andere van USB-sticks)								
	Verwijdering van onderdelen waardoor storingen ontstaan								
Programmatuur	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja//Nee/Nr**
Nalatig menselijk handelen	Ontwerp-, programmeer-, invoering, beheer/onderhoudsfouten								
	Introductie van virus en dergelijke door gebruik van niet gescreende programma's								
	Gebruik van de verkeerde versie van programmatuur								
	Slechte documentatie								
Opzettelijk menselijk	Manipulatie voor of na ingebruikname								

handelen	(Ongeautoriseerde) functieverandering en/of toevoeging								
	Installatie van virussen, Trojaanse paarden en dergelijke								
	Kapen van autorisaties van collega's								
	Illegaal kopiëren van programmatuur								
	Oneigenlijk gebruik of privé gebruik van bedrijfs programmatuur								
Onopzettelijk menselijk handelen	Fouten door niet juist volgen van procedures								
	Installatie van malware en virussen door gebruik van hoge autorisaties bijvoorbeeld door gebruik van admin-account tijdens het browsen van websites.								
Technische fouten/mankementen	Fouten in code programmatuur die de werking verstoren								
	Achterdeuren in programmatuur voor (onbevoegde) toegang								
	Bugs/fouten in code die tot exploits kunnen leiden								
Gegevens/data	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Via gegevensdragers (CD/DVD/ USB-ticks/ Harddisk/ Back-ups	Diefstal/zoekraken/lekken								
	Beschadiging door verkeerde behandeling								
	Niet overeenkomende bestandformaten								
	Foutieve of geen versleuteling								
	Foutieve of vervalste identificatie van ontvangers om aan gegevens te komen								

Via Cloud voorzieningen	Ongeautoriseerde toegang door onbevoegden (hackers/hosters)								
	Ongeautoriseerde wijziging of verwijdering van gegevens (hacking)								
Via apparatuur	Fysieke schrijf- of leesfouten								
	Onvoldoende toegangsbeperking tot apparatuur								
	Fouten in interne geheugens								
	Aftappen van gegevens								
Via programmatuur	Foutieve of gemanipuleerde programmatuur								
	Doorwerking van virussen/malware								
	Afbreken van verwerking								
Via personen	(On)opzettelijke foutieve gegevensinvoer, -verandering of –verwijdering van data								
	Onbevoegde toegang door onbevoegden (hackers en dergelijke via malware)								
	Onbevoegd kopiëren van gegevens								
	Meekijken over de schouder door onbevoegden								
	Onzorgvuldige vernietiging (laten liggen op printer)								
	Net toepassen clear screen/clear desk								
	Aftappen (draadloos) netwerk door onbevoegden (telewerk situaties)								
	Oneigenlijk gebruik van autorisaties								
	Toegang verschaffen door middel van								

	identiteitsfraude of social engineering								
	Onzorgvuldig vernietigen van gegevens								
Organisatie	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Gebruikersorganisatie	Mismanagement								
	Gebrekkige toedeling taken, bevoegdheden,								
	Verantwoordelijkheden								
	Onduidelijke of ontbrekende gedragscodes								
	Afwezige, verouderde of onduidelijke handboeken								
	Systeemdocumentatie / werkprocedures/ gebruiksinstructies								
	Onvoldoende interne controle								
	Onvoldoende toetsing op richtlijnen								
	Onvoldoende of geen contractbeheer								
	Ontbrekende of onduidelijke SLA's								
	Gebrekkige doel/middelen beheersing								
Beheerorganisatie	Gebrekkig beleid betreffende beheer								
	Onvoldoende kennis of capaciteit								
	Onvoldoende kwaliteitsborging								
	Onvoldoende beheer van systemen en middelen (ICT-Atlas)								
Ontwikkelingsorganisatie	Slecht projectmanagement								
	Niet volgen van projectenkalender of PPM								

	Geen ontwikkelrichtlijnen en/of – procedures								
	Er worden geen methoden/technieken gebruikt								
	Gebrek aan planmatig werken								
Omgeving	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Buitengebeuren	Natuurgeweld (overstroming, blikseminslag, storm, aardbeving et cetera)								
	Overig geweld (oorlog, terrorisme, brandstichting, inbraak, neerstortend vliegtuig, galactische oorlogsvoering)								
	Blokkade/staking								
	Onveilige, geblokkeerde, vluchtwegen bij brand								
Nutsvoorzieningen	Uitval van elektriciteit, water, telefoon								
	Wateroverlast door lekkage, bluswater								
	Uitval van licht-, klimaat- en/of sprinklerinstallatie								
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								
Diensten	**Incident**	**H**	**M**	**L**	**H**	**M**	**L**	**Ja/Nee**	**Ja/Nee/Nr.**
Diensten dienstverlener definitief niet meer te leveren	Een dienstverlener gaat failliet								
	Opzegging diensten door dienstverlener								

Diensten dienstverlener tijdelijk niet beschikbaar	Levert diensten niet conform overeenkomst								
	Onderbreking dienstverlening door overname dienstverlener								
	Kan diensten tijdelijk niet uitvoeren door zaken buiten de eigen controle (stakingen en dergelijke.)								
	Past verkeerde prioriteiten toe in klantbejegening								
	Levert onvoldoende capaciteit voor een goede dienstverlening								
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 geldig VOG en geheimhoudingsverklaringen								
	Voert wanbeheer, slordigheden in beheersactiviteiten,								
	Werkt niet conform ITIL of BiSL-principes								
	Maakt misbruik van toevertrouwde gegevens, applicaties en documentatie								
	Houdt zich niet aan functiescheiding								
	Maakt gebruik van te zware autorisatie, niet functie gebonden								