Titelpagina

Titel	Informatiebeveiliging
Subtitel	Vertrouwelijke informatie daadwerkelijk veilig?
Auteur	Etienne Nijs Weegbree 3 5803 LV Venray Nederland enijs@derooysewissel.nl etienne.nijs@gmail.com
Opleiding	Fontys Hogescholen ICT Bedrijfskundige Informatica
Afstudeerdocente	Mevr. Jolanda Liégeois Team Primair Proces HI
Organisatie	F.P.C. de Rooyse Wissel Wanssumseweg 12a 5807 EA Venray Nederland +31 (0) 478 635200 +31 (0) 478 635261 info@derooysewissel.nl
Bedrijfsmentor	Dhr. Guido Hillekens Hoofd I&A / Informatieanalist
Afstudeerperiode	20 september 2010 – 25 februari 2011
Datum	Venray, 03-03-2011

Versiebeheer

Versie	Datum	Bijzonderheden	Auteur
0.1	18-01-2011	1e opzet eindrapport	Etienne Nijs
0.2	02-02-2011	2e opzet na bespreking met stagedocente J. Liégeois	Etienne Nijs
0.3	16-02-2011	3e opzet na bespreking met bedrijfsmentor G. Hillekens	Etienne Nijs
1.0	28-02-2011	Definitieve versie van scriptie na goedkeuring	Etienne Nijs

Verzendlijst

Organisatie	Naam	Functie
F.P.C. de Rooyse Wissel	Guido Hillekens	Hoofd I&A / Informatieanalist
Fontys	Jolanda Liégeois	Afstudeerdocente
Fontys	Antonet Barten – van de Rijt	Administratief Medewerker IT

Voorwoord

In het kader van de studie Bedrijfskundige Informatica is binnen de Rooyse Wissel de mogelijkheid om een project uit te voeren dat naadloos aansluit op de studie BI. De theorie die tijdens de studie is opgedaan, zal tijdens het project in de praktijk worden toegepast.
Gedurende dit project wordt de informatiebeveiliging van F.P.C. de Rooyse Wissel getoetst aan de hand van een IT-audit. Samen met de informatiebeveiligingsfunctionaris worden de betrokken informatievoorzieningen geïdentificeerd en getoetst aan de norm voor informatiebeveiliging, die in de zorg gehanteerd wordt (NEN7510).

Een combinatie van verschillende methodieken vormen de leidraad binnen deze IT-audit. Deze methodes zullen als resultaat een risico- en maatregelenanalyse beschrijven, waarmee F.P.C. de Rooyse Wissel de informatiebeveiliging geheel op orde kan krijgen. Deze maatregelen zullen ook in de toekomst gewaarborgd worden aan de hand van het informatiebeveiligingsplan. Dit project zal een aanzet zijn voor de informatiebeveiligingsfunctionaris om de informatiebeveiliging in de toekomst te waarborgen. Dit zal onder anderen gedaan worden door jaarlijks een audit uit te voeren.

De verschillende methodes, resultaten en conclusies zijn verwerkt in dit rapport en zijn bedoeld als informatiebron, waardoor de organisatie alle informatie omtrent informatiebeveiliging in kaart heeft.

Graag wil ik F.P.C. de Rooyse Wissel bedanken voor de mogelijkheid om binnen deze organisatie te mogen afstuderen. De opdracht die mij geboden is sluit aan op de theorie die opgedaan is tijdens de studie Bedrijfskundige Informatica. Echter is het verschil tussen theorie en praktijk groter dan ik dacht. Uiteraard is de theorie van groot belang, maar het toepassen van deze theorie in de praktijk heeft mijn kennis en interesses zeer verbreed.
Graag wil ik ook Mevr. J. Liégeois, Dhr. R. van Stratum en Dhr. R. Hamers bedanken voor de toewijding en begeleiding die zij mij geboden hebben tijdens dit project. Daarnaast wil ik mijn bedrijfsmentor Dhr. G. Hillekens bedanken voor de begeleiding van de opdracht en Dhr. R. Leijssen bedanken voor de nauwe samenwerking die heeft geholpen dit project succesvol af te ronden. Tenslotte wil ik ook alle overige medewerkers binnen F.P.C. de Rooyse Wissel bedanken voor hun bijdrage en inzet.

Inhoudsopgave

Samenvatting

Informatiebeveiliging in de zorg is van essentieel belang. De Rooyse Wissel dient te voldoen aan de normen die gelden binnen deze sector. Aan de hand van een audit zijn de informatiesystemen en gegevensgebieden getoetst aan de geldende normen. De aanleiding van deze afstudeerstage is dat de awareness binnen de Rooyse Wissel op het gebied van informatiebeveiliging nog niet optimaal is. Door dit project zal informatiebeveiliging in de toekomst een vast punt op de agenda moeten worden, zodat vertrouwelijke informatie veilig op de informatiesystemen van de Rooyse Wissel verwerkt kan worden.
Dit rapport vat de afstudeerstage samen en is uiteindelijk samen met de presentatie de afsluiting van de studie Bedrijfskundige Informatica.

Het doel van deze opdracht is de huidige situatie van de Rooyse Wissel op het gebied van informatiebeveiliging goed in kaart te brengen. Een IT-audit is toegepast om dit doel te bereiken.

Aan de hand van verschillende literatuurstudies en kennisdeling van medewerkers van de afdeling Informatie en Automatisering is het project uitgevoerd. Er is ook gebruik gemaakt van verschillende bronnen op het internet. Verwijzingen naar al deze bronnen zijn te vinden in het hoofdstuk literatuuropgave.

De resultaten van de audit zijn door middel van verschillende analyses verkregen. De risicoanalyse is aan de hand van de A, B & K-methode uitgevoerd. De huidige situatie is getoetst door middel van een GAP-analyse. De GAP is het verschil tussen de werkelijke en wenselijke situatie. Een checklist op basis van de NEN7510 norm wordt ingevuld om deze GAP te bepalen. De resultaten die uit deze analyses voortvloeien zijn de meest relevante bedreigingen en risico's, de maatregelen die genomen moeten worden om te voldoen aan de geldende norm en de maatregelen die genomen moeten worden om de risico's te beperken en/of uit te kunnen sluiten. In de bijlage zijn alle resultaten opgenomen.

Is de informatiebeveiliging binnen F.P.C. de Rooyse Wissel voldoende op orde, om ongewenste schade te voorkomen? Aan de hand van verschillende resultaten kan deze vraag positief beantwoord worden. Op het gebied van fysieke- en toegangsbeveiliging voldoet de Rooyse Wissel uitstekend aan de normen die gesteld zijn. Echter zijn op het gebied van bijvoorbeeld beveiligingseisen t.a.v. het personeel en het operationeel beheer van informatievoorzieningen, enkele eisen die absoluut moeten worden aangescherpt. De focus zal zich in de nabije toekomst vooral moeten richten op beleidsstukken en procedures. Op een aantal gebieden zijn deze documenten niet beschreven, waardoor er geen concrete regels zijn. Over het algemeen voldoet de Rooyse Wissel voldoende aan de gestelde eisen binnen het normkader, maar er zal wel rekening gehouden moeten worden met de relevante risico's die aan de hand van de analyses zichtbaar zijn geworden.

Voor een uitgebreide uitleg en onderbouwing van bovenstaande informatie verwijs ik u naar de inhoud van dit verslag.

Summary

Information security in healthcare is essential. De Rooyse Wissel must comply with the standards applied in this sector. The information systems and data areas will be assessed to these standards by using an audit. The goal of this internship is to improve the awareness of information security within the Rooyse Wissel. Through this project, information security must become a permanent item on the agenda of all employees so that confidential information can be processed safely on the information systems of the Rooyse Wissel.
This report summarizes the internship. The report and a presentation will be the final stage of the study Business Intelligence.

The goal of this project is to chart the current status of information security of the Rooyse Wissel. An IT-audit is used to achieve this goal.

Based on various literature studies and the knowledge of employees from the IT department, the project has been executed. Also various sources on the internet are used. References to these sources can be found in the chapter 'literatuuropgave'.

The audit results are obtained by using different analyses. The risk analysis is done according to the A, B & K-method. The current status of information security is reviewed by using the GAP-analysis. The GAP is the difference between the current situation and the desirable situation. A checklist, according to the NEN7510 standard, is used to determine the GAP. The results from these analyses are the most relevant threats and risks, the measures to be taken to meet the current standard and the measures to be taken to reduce or eliminate these risks. See the appendix for the overall results.

Is the security of information within the Rooyse Wissel sufficiently in order to avoid unwanted damage? Based on several results, this question can be answered positively. In terms of physical and access control the Rooyse Wissel meets the requirements perfectly, according to the standards. However, some requirements need to be improved in terms of security requirements of personnel and the operational management of information systems. The main target for the near future should focus on the policy documents and procedures. In some areas these documents are not described, which means there are no concrete rules.
Generally, the Rooyse Wissel meets the requirements within the standard sufficiently, but the Rooyse Wissel will have to take account with the relevant risks which are identified within the analysis.

For a detailed explanation of the above information, please see the content of this report.

Verklarende woordenlijst

A, B & K-analyse	Afhankelijkheids-, bedreigingen- en kwetsbaarheidsanalyse, een methode om risico's en bijbehorende kwetsbaarheden te identificeren.
Awareness	De mate van bewust zijn onder de medewerkers.
Back Office	De Back Office is onderdeel van de afdeling Informatie en Automatisering die ondersteuning biedt aan de dienstverlening.
BI	Bedrijfskundige Informatica, opleiding met een breed praktijkgericht vakgebied waarin men kennis en vaardigheden ontwikkelt op het terrein van bedrijfskunde en informatica.
BIV	Beschikbaarheid, integriteit en vertrouwelijkheid, aspecten die de betrouwbaarheid van informatie aangeven.
BSP-methode	Business System Planning, methode voor afstemming van informatievoorziening op de verschillende bedrijfsprocessen.
F.P.C.	Forensisch Psychiatrisch Centrum, instituut ter verpleging en/of behandeling van, overwegend, tbs patiënten binnen een beveiligd kader.
Front Office	De Front Office is het deel van de afdeling Informatie en Automatisering dat in rechtstreeks contact staat met de overige afdelingen. Ook wel servicedesk genoemd.
I&A	Informatie en Automatisering, afdeling binnen F.P.C. de Rooyse Wissel waar de stagiair zal werken aan het project.
Informatie	Voor processen betekenisvolle gegevens, die door deze processen worden gebruikt, bewerkt of verwerkt.
Informatiekruis	Schematische samenvatting van het verband tussen bedrijfsprocessen, afdelingen, gegevensgebieden en informatiesystemen.
INK-model	Een breed gebruikt managementmodel dat bedoeld is voor organisaties om een zelfevaluatie uit te voeren.
IT-audit	De onafhankelijke en deskundige beoordeling van kwaliteitsaspecten van informatiesystemen.
NEN7510	De norm NEN 7510 gaat over informatiebeveiliging binnen de zorgsector.
NOREA	Beroepsorganisatie van IT-auditors in Nederland
PvA	Plan van Aanpak, rapport waarin de aanpak van een project beschreven is.
Quickscan	Toetsing aan de hand van een standaard vragenlijst.
TBS	Terbeschikkingstelling, maatregel die een delictpleger opgelegd kan krijgen.

1. Inleiding

Voldoet de informatiebeveiliging van F.P.C. de Rooyse Wissel aan de normen die gelden voor deze sector?
Deze vraag staat centraal in dit verslag. Aan de hand van een IT-audit kan er antwoord gegeven worden op deze vraag en zullen de risico's en maatregelen zichtbaar worden.

1.1 Achtergrond Informatie

Tijdens de studie Bedrijfskundige Informatica leer je ICT toe te passen in organisaties om bedrijfsprocessen en informatiesystemen te verbeteren. Analyseren, beschrijven en verbeteren van processen zijn de kernwerkzaamheden van een BI-er. Hiervoor dient men een goed inzicht te hebben in de organisatie, de communicatielijnen, informatiestromen en de informatiebehoeften. ICT speelt hierin een belangrijke rol zonder dat de techniek van computers centraal staat.
De BI-er werkt nauw samen met de gebruikers van informatiesystemen en vervult vaak een brugfunctie tussen de gebruikers, het management en de beheerders van informatiesystemen.
Zowel het bedrijfskundige als het informatica deel van de opleiding is betrokken binnen het project. Enerzijds vindt een bedrijfskundig onderzoek plaats om inzicht te krijgen in de organisatie. De informatieanalyse loopt parallel aan het bedrijfskundige onderzoek en deze beschrijft de informatiesystemen, processen en gegevensgebieden. De uitkomst van de informatieanalyse wordt verwerkt in de IT-audit. Deze manier van werken vormt de leidraad in de studie Bedrijfskundige Informatica.

1.2 Bedrijfsbeschrijving

Wat is F.P.C. de Rooyse Wissel precies? Hoe ziet de organisatie van F.P.C. de Rooyse Wissel eruit? In deze paragraaf wordt een korte indruk gegeven. Tevens is de afdeling beschreven waarbinnen het project is uitgevoerd.

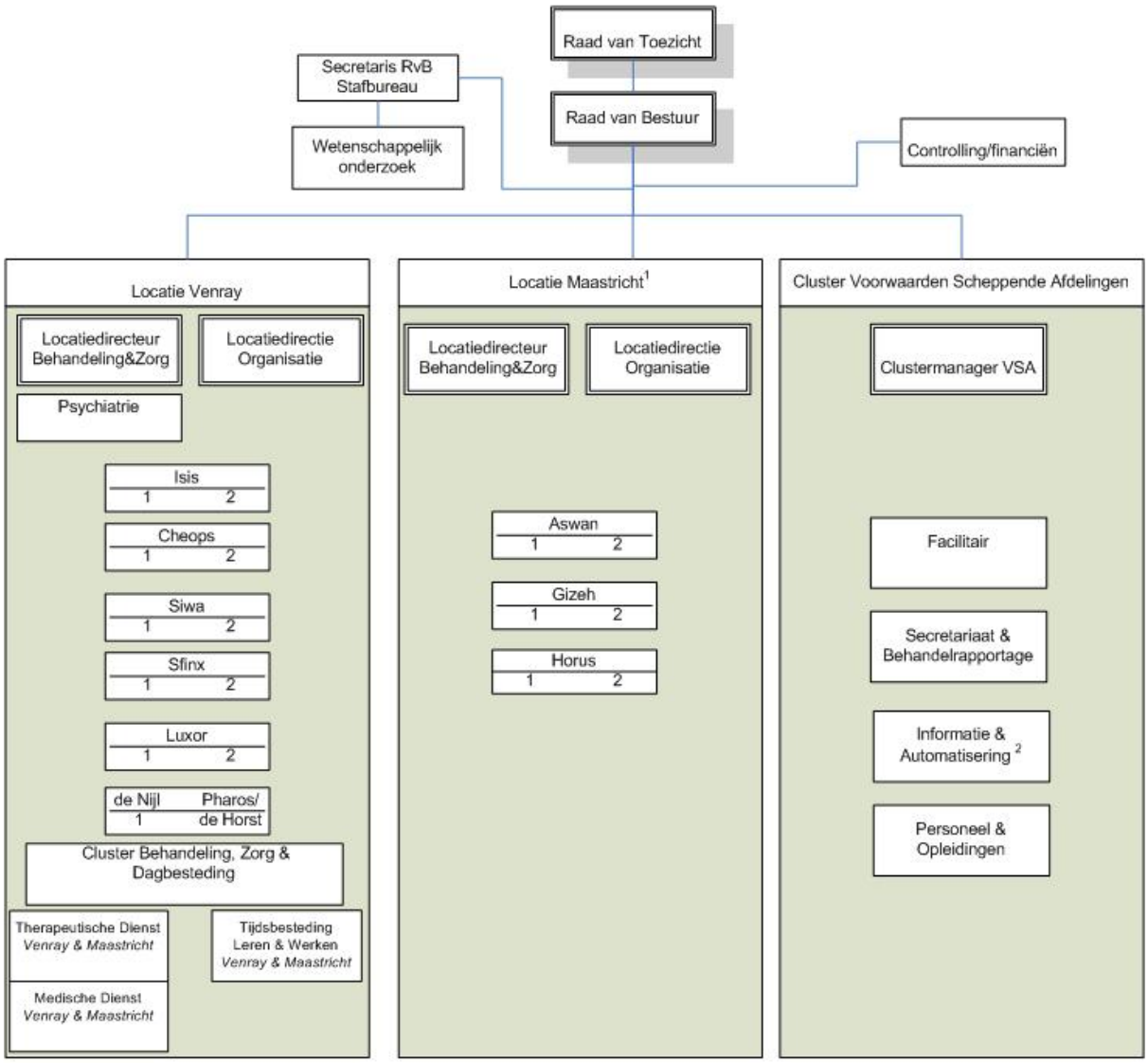
De Rooyse Wissel is een particulier forensisch psychiatrisch instituut ter verpleging en/of behandeling van, overwegend, tbs patiënten binnen een beveiligd kader. De Rooyse Wissel heeft een gebouw dat er qua beveiliging van de buitenkant uitziet als een gevangenis. Binnen is het echter een licht en vriendelijk aandoende kliniek waar geen bewakers met uniformen en sleutels rondlopen.
Het is de enige Tbs-kliniek in het zuiden van het land en er worden alleen mannelijke TBS-patiënten behandeld. De Rooyse Wissel is een particuliere kliniek. Dat wil zeggen dat het beheer, de exploitatie en het behandelbeleid een verantwoordelijkheid is van het bestuur van de Stichting Tbs-kliniek Venray.

F.P.C./P.P.C. Overmaze in Maastricht is ook onderdeel van de Rooyse Wissel. Overmaze is zowel een Penitentiair Psychiatrisch Centrum (P.P.C.) als een Forensisch Psychiatrisch Centrum (F.P.C.). De PI Limburg Zuid draagt zorg voor de facilitaire zaken en de beveiliging en F.P.C. de Rooyse Wissel voor het zorginhoudelijke programma en de medewerkers.

Sinds kort is de Rooyse Wissel een samenwerkingsverband aangegaan met de Ottho Gerhard Heldringstichting (OGH) te Zetten. De OG Heldringstichting is een particulier behandelcentrum voor observatie, verzorging, opvoeding, behandeling en begeleiding van jongeren met ernstige en gecompliceerde gedragsproblemen.

1.2.1 Stagebedrijf

Organogram



Figuur 1: Organogram de Rooyse Wissel

Binnen F.P.C. de Rooyse Wissel zijn momenteel ongeveer 500 medewerkers werkzaam. Hier tegenover staan 227 patiënten. De relatie is dus ongeveer 2:1.

Missie

Het doel van de Rooyse Wissel is het tot maatschappelijk aanvaardbaar niveau terugbrengen van het delictgevaar, met als streven terugkeer of handhaving van de patiënt in de maatschappij. De Rooyse Wissel staat tevens voor het verlenen van ambulante zorg aan forensisch psychiatrische patiënten en het, in samenwerking met relevante partners, uitwisselen en verzamelen van expertise.
Bron: http://www.derooysewissel.nl

Behandelvisie
Het uiteindelijke doel van de behandeling is dat de patiënt weer terugkeert in de maatschappij zonder (ernstige) delicten te plegen. De patiënt moet, ook in moeilijke situaties, controle hebben over zijn eigen gedrag. Om dit te bereiken wordt niet alleen aan het gedrag van de patiënt gewerkt, maar ook aan de onderliggende stoornis. Behandeling van welke stoornis dan ook zal slechts dan plaatsvinden als er een causaal verband bestaat tussen de stoornis en het delict. Uiteraard is een terugkeer in de vrije maatschappij niet voor iedere patiënt weggelegd. Wel moet gekeken worden of het hoge beveiligingsniveau van de Tbs-kliniek voortdurend nodig is, of dat een setting met een geringer beveiligingsniveau kan volstaan. Voor sommige patiënten betekent dit dan ook dat ze uiteindelijk terugkeren in de vrije maatschappij, voor anderen is dit niet haalbaar en zal gezocht moeten worden naar een passende vervolgvoorziening.
Bron: http://www.derooysewissel.nl

Resultaatgericht
De basis van De Rooyse Wissel wordt gevormd door haar Missie en haar Visie.
Naast haar missie en visie, baseert de kliniek haar organisatie op een zestal besturingsinstrumenten. Voor het besturen van de organisatie maakt de Rooyse Wissel gebruik van de planning & control-cyclus, kwaliteitsmanagement (INK-model) en competentiemanagement.
Hiermee bewerkstelligt het instituut dat het een op kwaliteit en resultaat en dus op output, of zelfs outcome, gerichte organisatie is.
Bron: http://www.derooysewissel.nl

1.2.2 Plaats binnen de organisatie

Het project is uitgevoerd binnen de afdeling Informatie & Automatisering (I&A). I&A zorgt ervoor dat de informatiesystemen binnen de Rooyse Wissel te allen tijde draaiende blijven. Aan de hand van een Front Office (servicedesk en systeembeheer) en Back Office (applicatiebeheer, informatiebeheer en technisch beheer) worden de technische informatiesystemen beheerd en onderhouden.

1.3 Probleemstelling

Informatiebeveiliging is binnen elke organisatie van groot belang. In de forensische psychiatrische centra is de informatie van levensbelang. Gegevens over patiënten, medicatie en beveiliging mogen absoluut niet in de handen komen van bijvoorbeeld kwaadwillenden. Het uitlekken van informatie binnen deze branche kan dus zorgen voor imagoschade en de daarbij betrokken financiële consequenties.

Door middel van een audit op de informatiesystemen, kunnen de risico's op het gebied van informatiebeveiliging herkend en beschreven worden. Aan de hand van deze risicoanalyse zullen een aantal maatregelen beschreven worden, die mee worden genomen in het informatiebeveiligingsplan. Met behulp van dit plan zullen de risico's in de toekomst beperkt blijven en zullen de maatregelen gewaarborgd worden.

De vraag waar dit project antwoord op dient te geven:

"Is de informatiebeveiliging binnen F.P.C. de Rooyse Wissel voldoende op orde, om ongewenste schade te voorkomen?"

1.4 Doelstelling

De informatiebeveiliging toetsen aan de gelden normen, om zo de mogelijke risico's te identificeren. Waarborgen van de hierdoor ontstane noodzakelijke maatregelen, om gegevensverlies en uiteindelijk ook imago- en financiële schade te voorkomen.

1.5 Grenzen/Beperkingen

In eerste instantie is de informatiebehoefte binnen F.P.C. de Rooyse Wissel gevestigd op de IT-audit. De IT-audit zal centraal op de locatie Venray worden uitgevoerd. Het identificeren van de betrokken systemen, belangrijkste processen, normeringen en het uitvoeren van een risicoanalyse staan in dit project centraal. De informatie die uit deze onderzoeken voortkomt, wordt in een auditrapport verwerkt.

De scope van de audit is gevestigd op het kwaliteitsaspect vertrouwelijkheid. Dit aspect is van belang voor de informatiebeveiliging. De kwaliteitsaspecten beschikbaarheid en integriteit zijn buiten de scope van het project gehouden. De informatie die voor deze aspecten verwerkt dient te worden, is te veel in verhouding tot de tijd die beschikbaar is voor het project. Deze aspecten zijn op organisatorisch niveau natuurlijk wel van belang, maar zullen in een volgend stadium pas worden uitgewerkt.

De overdracht van de projectresultaten sluit het project af en is de basis voor een aansluitend project, zodat de informatiebeveiligingsfunctionaris het informatiebeveiligingsplan kan uitwerken en de maatregelen zal waarborgen in de toekomst. Het informatiebeveiligingsplan opstellen en de daarop volgende fases vallen buiten de scope van dit project.

1.6 Leeswijzer

In hoofdstuk 2 zal eerst ingegaan worden op de methodieken die gebruikt zijn om de onderzoeken uit te voeren. In hoofdstuk 3 zijn de resultaten opgenomen die aan de hand van de verschillende onderzoeken verkregen zijn. In hoofdstuk 4 zijn de conclusies beschreven die getrokken zijn aan de hand van het project. Verder zijn in dit hoofdstuk de aanbevelingen meegenomen en is er een conclusie getrokken over de gebruikte methodes. Tot slot voorziet hoofdstuk 5 in een literatuuropgave en zijn de bijlagen opgenomen in hoofdstuk 6.

2. Onderzoeksmethode

Om de projectopdracht zo goed mogelijk uit te voeren, kan er gebruik gemaakt worden van verschillende methoden. De methoden die tijdens dit project aangehouden zijn, zullen in dit hoofdstuk besproken worden.
Om de kwaliteit van de projectopdracht en bijbehorende producten te kunnen waarborgen, is er o.a. gebruik gemaakt van de literatuur “Informatiebeveiliging onder controle”. Verder is er ook gebruik gemaakt van literatuur over projectmanagement, IT-auditing en de handreiking van NOREA (beroepsorganisatie van IT-auditors in Nederland).

2.1 Algemeen

Om de voortgang van het project te kunnen bewaken, zullen er wekelijks voortgangsbesprekingen plaatsvinden. Tijdens deze bespreking, worden de projectactiviteiten toegelicht. Hiernaast zal ook een aangepast planning besproken worden.
De kwaliteit van het projectresultaat zal intern bewaakt worden door tussentijdse voortgangsbesprekingen. Externe controles zullen worden uitgevoerd door de afstudeerdocent. Aan de hand van logboeken, kan deze docent exact zien welke activiteiten zijn uitgevoerd.

Om gegevensverlies te voorkomen, door bijvoorbeeld een crash op het werkstation, worden alle documenten gesynchroniseerd met de server. De server maakt dagelijks, wekelijks, maandelijks en jaarlijks back-ups. Om inzicht te krijgen in de wijzigingen die doorgevoerd zijn bij het opstellen van de documentatie, is gebruik gemaakt van versiebeheer.

Het plan van aanpak is opgesteld volgens de projectmanagement methode van Roel Grit. Deze methode wordt voornamelijk in het hoger beroepsonderwijs en universitair onderwijs toegepast. De methode werkt volgens een bepaalde fasering om de beheersbaarheid van het project te vergroten. De basis van deze fasering is het maken van een PvA. Ook het PvA volgens Grit heeft een structurele opzet. Het PvA van dit project is aangevuld met een risicoanalyse en kosten-/baten overzicht volgens ‘Grit, R. (2005) *Projectmanagement’.*

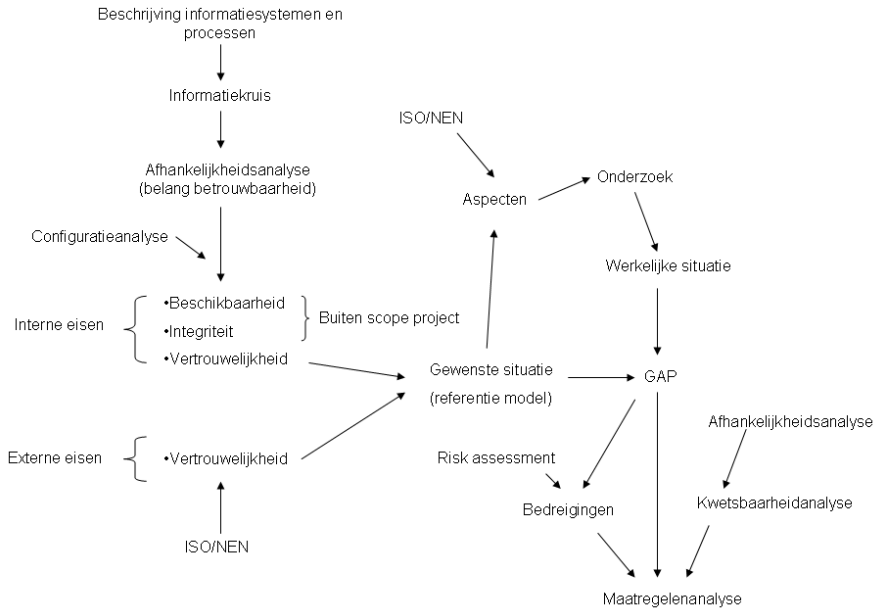
2.2 IT-audit

IT-auditing is het vakgebied dat zich bezighoudt met het beoordelen van de automatisering van de organisatie en de organisatie van de automatisering. Organisaties willen in toenemende mate zekerheid over de betrouwbaarheid en beveiliging van hun geautomatiseerde informatievoorzieningen. Met name de financiële systemen en de grotere automatiseringsprojecten worden daarom periodiek beoordeeld door IT auditors.

De evaluatie van het verkregen bewijs bepaalt of de informatiesystemen werken naar behoren, de beschikbaarheid, integriteit en de vertrouwelijkheid van de gegevens gewaarborgd worden en de effectiviteit waarin de organisatie de doelstellingen bereikt.

Om de IT-audit naar behoren uit te voeren, is er onderzoek gedaan naar de verschillende methodes. Deze methodes zijn gezamenlijk verantwoordelijk voor de kwaliteit van de gehele audit.

Om duidelijk te maken welke weg bewandeld is gedurende de IT-audit, is een project activiteitenschema opgesteld. Onderstaande figuur geeft wat meer duidelijkheid in de verschillende activiteiten die uitgevoerd zijn:

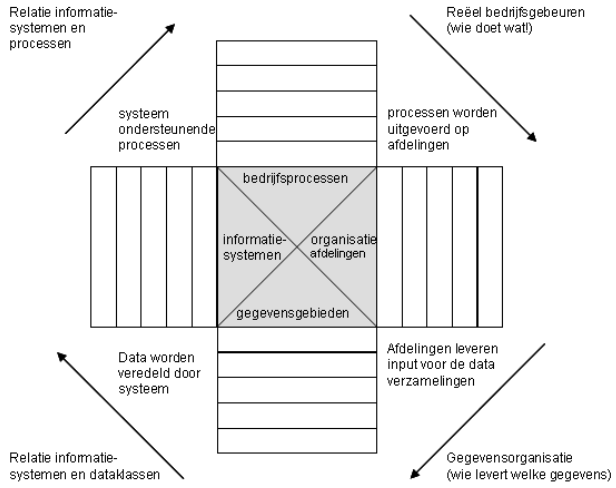


Figuur 2: Project activiteitenschema

De verschillende methodes uit het project activiteitenschema zijn in de aankomende subparagrafen verder uitgediept.

2.2.1 BSP-methode

De BSP-methode staat voor Business System Planning en is vooral bedoeld om de informatievoorziening beter af te stemmen op de diverse bedrijfsprocessen. Zeer kort samengevat kun je zeggen, dat bedrijfsprocessen uitgevoerd worden in een of meer afdelingen van een organisatie. Die afdelingen leveren input voor een bij te houden gegevensverzameling (database). Vervolgens kunnen die gegevens door informatiesystemen zodanig verwerkt worden, dat het uitvoeren van de bedrijfsprocessen effectief ondersteund kan worden. Dit is geheel schematisch samengevat in het onderstaande ‘informatiekruis’.



Figuur 3: Informatiekruis

Het informatiekruis wordt gebruikt om het directe verband aan te geven tussen informatie, systemen, organisatie en processen.

Het informatiekruis laat in een opslag zien:

- Verband tussen informatiesystemen en bedrijfsprocessen
- Verband tussen bedrijfsprocessen en de afdelingen
- Verband tussen de afdelingen en de gegevensgebieden
- Verband tussen de gegevensgebieden en de informatiesystemen

Onderstaand een voorbeeld van het verband tussen gegevensgebieden en informatiesystemen:

E	D	C	B	A	bedrijfsprocessen / informatie-systemen / organisatie afdelingen / gegevensgebieden
	C	U	U		klanten
	U	C		U	orders
	U	U		C	artikelen
C			U	U	grondstoffen

C = Create
U = Use

Figuur 4: voorbeeld gedeelte informatiekruis

In dit voorbeeld is duidelijk te zien welke gegevensgebieden verband hebben met welke informatiesystemen. Er wordt wel een verschil gemaakt tussen het aanmaken van de gegevens en het gebruik ervan. Dit is aangeduid als ‘create’ en ‘use’.

2.2.2 Risicoanalyse

Een IT-audit bestaat uit een aantal belangrijke onderdelen. Een van de belangrijkste onderdelen van een audit is de risicoanalyse. Risicoanalyse is een methode die informatie oplevert, waarmee het management in staat wordt gesteld te beslissen welke risico's, of welke combinatie van risico's, een grote potentiële schade vormen en met welke maatregelen deze risico's teruggedrongen kunnen worden.

Verschillende soorten risicoanalyses

Er bestaan verschillende soorten risicoanalyses:

- Quickscan
- Baseline checklist
- Kwalitatieve risicoanalyse
- Kwantitatieve risicoanalyse

Elk van deze risicoanalyses hebben voor- en nadelen. Deze voor- en nadelen zijn naast elkaar gelegd, om zo de meest geschikte analyse te selecteren.

Voor- en nadelen

Quickscan
Bij de quickscan wordt gebruik gemaakt van externe vragenlijsten. Hierbij dient er aan de algemene normen te voldoen.

Baseline checklist
De baseline checklist biedt meer diepgang. Hierbij wordt door middel van checklists geverifieerd of al dan niet aan de eigen baseline wordt voldaan. Deze baseline is een stelsel van eigen (of overgenomen) beveiligingsmaatregelen (de norm) die in de gehele organisatie wordt gevoerd.

Onderstaande voor- en nadelen gelden voor de quickscan en de baseline checklist.

+ *Eenvoud*, de toepassing van checklists is rechttoe rechtaan en vergt weinig mankracht. Voor het inzetten van een bestaande checklist is slechts één deskundige nodig.
  Normeerbaar, indien in meerdere situaties of locaties dezelfde checklist gebruikt wordt, dan zijn de resultaten vergelijkbaar en te toetsen aan de norm.
- *One size does not fit all*, de beveiligingsbehoeften van verschillende organisaties vertonen onderling vaak minder gelijkenis dan men op grond van andere overeenkomsten zou verwachten.
  Checklists zijn statisch, door snelle ontwikkelingen van de informatietechnologie is een checklist op het gebied van informatiebeveiliging vaak binnen afzienbare tijd verouderd.
  Hackers houden van checklists, een checklist kan in de handen van een tegenstander een gevaarlijk wapen zijn. Wie over een checklist beschikt die in een bepaalde organisatie gebruikt wordt, weet immers welke beveiligingsmaatregelen binnen die organisatie omzeild moeten worden.

Kwalitatieve risicoanalyse
Bij deze vorm van risicoanalyse worden de risico's geschat. Dit is de lichtste vorm van risicoanalyse waarbij daadwerkelijke sprake is van het analyseren van risico's.

Kwantitatieve risicoanalyse
De kwantitatieve risicoanalyse, waarbij de risico's waar mogelijk gekwantificeerd zijn in meetbare criteria, meestal geld. Dit is de meest uitgebreide en gedetailleerde vorm van risicoanalyse.

Onderstaande voor- en nadelen gelden voor de kwalitatieve en kwantitatieve risicoanalyse.

+ *Maatwerk*, informatiebeveiliging is en blijft maatwerk, waarbij checklists weliswaar nuttig kunnen zijn, maar niet voldoende. Risicoanalyse kan dit gat opvullen.
Up-to-date, aangezien een risicoanalyse voor iedere situatie opnieuw uitgevoerd wordt, is het relatief eenvoudig om afstemming te creëren met nieuwe ontwikkelingen op het gebied van informatietechnologie, de organisatie en de omgeving.

- *Complex*, het uitvoeren van een risicoanalyse is een tijdrovende klus, die bovendien veel expertise vereist. Dit geldt voor de kwantitatieve risicoanalyse nog meer dan voor de kwalitatieve risicoanalyse. Het uitvoeren van een risicoanalyse wordt hierdoor relatief duur.
Informatie-overload, door de uitgebreide en gedetailleerde aanpak kunnen risicoanalyses leiden tot een teveel aan informatie, waardoor het nemen van beslissingen niet makkelijker, maar juist moeilijker wordt.

Keuze

De keuze voor de inzet van een bepaald type risicoanalyse is afhankelijk van vele factoren. Het heeft bijvoorbeeld geen nut om een relatief zware methode risicoanalyse in te zetten als de organisatie daar niet aan toe is.
Als we kijken naar de voor- en nadelen van de behandelde risicoanalyse methodes is er eigenlijk maar één die binnen de scope van het project past. Eerst zullen de afgevallen methodes aan bod komen.

Quickscan
Naast de veelzeggende nadelen van de methode, is ook de gehele methode niet van toepassing. De quickscan is een 'scan' die in het kort het systeem 'bekijkt' en hier een rapportage over uitbrengt. Deze methode is voor dit project te simpel.

Baseline checklist
Soortgelijke methode als de quickscan, alleen met een iets grotere diepgang. Omdat deze methode ook o.a. met checklists werkt, zijn de nadelen van de methode te groot om uit te voeren voor dit project.

Kwantitatieve risicoanalyse
Door deze uiterst gedetailleerde methode zal het project veel tijd in beslag nemen en vooral doelen op de financiële kant van de risico's. De complexiteit van de methode zal niet in het tijdsbestek van het project passen.

De gekozen methode is de ***kwalitatieve risicoanalyse***.

Deze methode past het beste bij de scope van het project, omdat dit de lichtste vorm van risicoanalyse is waarbij daadwerkelijk sprake is van het analyseren van de risico's. Dit wil zeggen dat deze methode binnen het tijdsbestek past en het beste aansluit bij de organisatie. Doordat het maatwerk betreft, zal de analyse aangepast worden aan het systeem. Geen standaardvragen uit een checklist, maar onderzoeken die daadwerkelijk op maat zijn gemaakt voor de organisatie.

2.2.3 A, B & K-analyse

De A, B & K-analyse is een analyse in het kader van risicomanagement. Ook wel de afhankelijkheids-, bedreigingen- en kwetsbaarheidsanalyse genoemd. Zoals de naam al zegt, wordt er onderzoek gedaan naar de afhankelijkheden, bedreigingen en kwetsbaarheden van de informatievoorzieningen. De A, B & K-analyse is afgeleid van de A & K-analyse, die misschien wat beter bekend is. In het boek *'informatiebeveiliging onder controle'* is deze A & K-analyse uitgewerkt.

Afhankelijkheidsanalyse:
"Het vaststellen in hoeverre en in welke mate de door de informatievoorziening ondersteunde bestuurs- en bedrijfsprocessen afhankelijk zijn van de betrouwbaarheid van de informatievoorziening en het vaststellen welke potentiële gevolgen kunnen optreden als gevolg van storingen in de informatievoorziening."

Bedreigingenanalyse:
"Het identificeren van de bedreigingen (ongewenste gebeurtenissen) waaraan de informatievoorziening bloot staat."

Kwetsbaarheidanalyse:
"Het vaststellen van de invloed van bedreigingen op het functioneren van de informatievoorziening."

3. Resultaten

3.1 Identificatie informatiesystemen

De verschillende informatiesystemen en IT-middelen binnen de Rooyse Wissel zijn geïdentificeerd en op papier gezet. Deze informatie is verkregen door middel van een aantal interviews met de systeembeheerder, de informatiebeveiligingsfunctionaris en het Hoofd I&A.

In deze beschrijving maken we onderscheid in een aantal onderwerpen:

- Software
- Hardware
- Back-up
- Netwerk
- Fysieke locaties
- Gegevensuitwisseling via bestanden

Voor de beschrijving van deze informatiesystemen, verwijs ik u door naar bijlage II

3.2 Beschrijving processen

Om de informatiebehoefte van het project te realiseren zijn alle belangrijkste processen beschreven. De processen die meegenomen worden, zijn bepaald door het Hoofd I&A. Om aan de juiste informatie te komen, zijn de proceseigenaren van de verschillende processen geïnterviewd. Per proces zijn de ondersteunende informatiesystemen, de afhankelijkheid van het informatiesysteem ten behoeve van het proces, de taken binnen het proces en de afdelingen waar het proces wordt uitgevoerd, beschreven.

Onderstaand een schema met processen die onder de loep zijn genomen:

Proces	**Eigenaar**
Behandelen	Hoofd Behandeling
Zorginkoop	Locatie Directie
DBBC registratie	Controller
Facturatie	Hoofd Financiën
Planning	Locatie Directie
Personeel	Hoofd P&O
Sturen	Secretaris Raad van Bestuur
Inkoop	Hoofd Facilitaire Dienst
Boekhouding	Hoofd Financiën

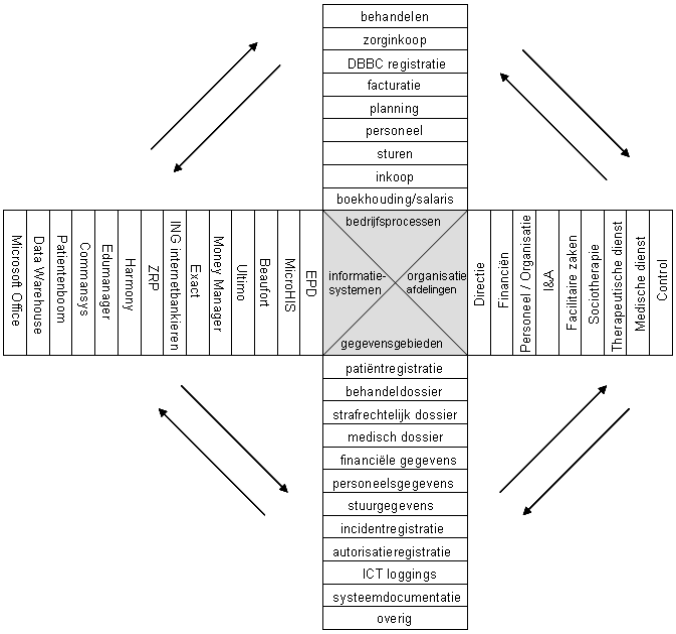
De resultaten van dit onderzoek zijn verwerkt in het informatiekruis. De procesbeschrijvingen zijn in bijlage III meegenomen.

In de volgende paragraaf wordt er verder gekeken naar het informatiekruis.

3.3 Informatiekruis

Met behulp van het informatiekruis worden de processen, informatiesystemen, gegevensgebieden en afdelingen in één schema duidelijk weergegeven. Tevens zijn de verbanden tussen deze onderdelen in kaart gebracht. De processen en informatiesystemen zijn uit het resultaat van de voorgaande onderzoeken meegenomen. De gegevensgebieden die tevens in het informatiekruis zijn opgenomen komen uit het informatiebeveiligingsbeleid. De afdelingen die zijn opgenomen in het informatiekruis zijn bepaald aan de hand van de processen, informatiesystemen en de gegevensgebieden. Het verband tussen het proces en het informatiesysteem is van belang voor de afhankelijkheidsanalyse.

Onderstaand een figuur van het informatiekruis met de verschillende onderdelen:



Figuur 5: Ingevuld informatiekruis

Voor de complete versie van het informatiekruis verwijs ik u door naar bijlage IV.

3.4 Afhankelijkheidsanalyse

Het doel van de afhankelijkheidsanalyse is het bepalen in hoeverre het proces afhankelijk is van het informatiesysteem. Aan de hand van het belang van het informatiesysteem en het belang van het proces is het belang van betrouwbaarheid berekend per kwaliteitsaspect.

Onderstaande figuur geeft hier wat duidelijkheid in:

		Informatiesysteem		
Proces		**Beschikbaarheid**	**Integriteit**	**Vertrouwelijkheid**
	Belang informatiesysteem (B1)	***Beschikbaarheid (proces, systeem)	Integriteit (informatiegebied)	Vertrouwelijkheid (informatiegebied)
	Belang proces (B2)	Belang proces	Belang proces	Belang proces
	Belang betrouwbaarheid	****B3 = B1xB2	**B3 = B1xB2	**B3 = B1xB2

* Beschikbaarheid wordt bepaald door de afhankelijkheid van het proces t.a.v. het systeem. Oftewel kan het proces zonder systeem doorgang vinden.
** Zie matrix

Aan de hand van onderstaande matrix kan het belang van de betrouwbaarheid bepaald worden:

		Belang van het proces			
		Vitaal	*Nuttig*	*Support*	*Overbodig*
Belang van het informatiesysteem	*Zeer hoog*	E	B	W	G
	Hoog	B	W	G	G
	Gemiddeld	W	G	G	G
	Laag	G	G	G	G

E = Essentieel, B = Belangrijk, W = Wenselijk, G = Geen criterium

Voor het proces 'behandelen' is de volgende afhankelijkheidsanalyse opgesteld:

Proces		**Informatiesysteem**					
		EPD	**MicroHis**	**Patiëntenboom**	**PC**	**Server**	**Netwerk**
Behandelen	Belang IS (B, I, V)	Z,Z,Z	Z,Z,Z	H,Z,Z	Z, Z, Z	Z, Z, Z	Z, Z, Z
	Belang proces	V	V	V	V	V	V
	Belang Betrouwbaarheid (B, I, V)	E,E,E	E,E,E	B,E,E	E,E,E	E,E,E	E,E,E

De score voor de beschikbaarheid is verkregen uit de interviewresultaten van de verschillende proceseigenaren. Hierbij is gekeken naar de mate waarin het informatiesysteem van belang is voor het proces. De integriteit is bepaald door het gegevensgebied dat verwerkt wordt door het systeem en is verkregen door een interview met het Hoofd I&A. Denk bijvoorbeeld aan medische gegevens. Het is van groot belang dat deze gegevens integer zijn en niet ongewenst gemuteerd worden, om de daarbij komende (grote) gevolgen te voorkomen. De vertrouwelijkheid is tevens bepaald door het gegevensgebied dat verwerkt wordt in het informatiesysteem. Denk hierbij bijvoorbeeld aan patiëntgerelateerde gegevens die absoluut niet op straat mogen belanden. Dus in hoeverre is de informatie vertrouwelijk?

Het belang van het proces heeft een score gekregen op basis van de mate waarin het proces van belang is voor de bedrijfsvoering. De verschillende scores zijn:

- Vitaal: onontbeerlijk voor bedrijfsvoering
- Nuttig: belangrijke ondersteuning voor bedrijfsvoering
- Support: kan eventueel gemist worden
- Overbodig: kan goed gemist worden

Voor het bepalen van de uiteindelijke scores is het Hoofd I&A geraadpleegd.

Het belang van de betrouwbaarheid kan nu berekend worden aan de hand van de bovenstaande matrix. Het resultaat is de betrouwbaarheid gebaseerd op de beschikbaarheid, integriteit en vertrouwelijkheid.

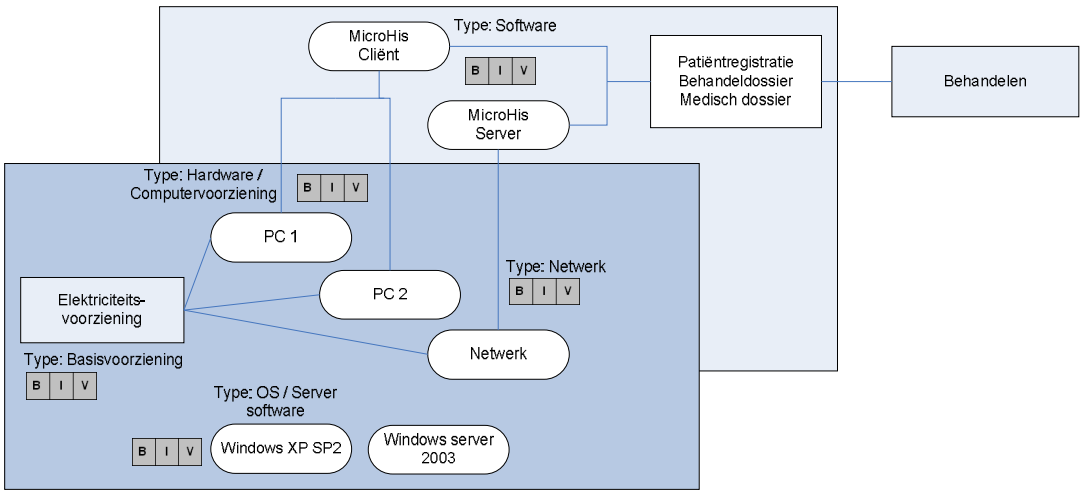
Voor de complete afhankelijkheidsanalyse verwijs ik u door naar bijlage V.

Aan de hand van de afhankelijkheidsanalyse, zal de configuratieanalyse worden uitgevoerd. De configuratieanalyse wordt in het volgende paragraaf besproken.

3.5 Configuratieanalyse

Een configuratieanalyse heeft tot doel te bepalen hoe een informatiesysteem (of een deel ervan) opgebouwd is en welke betrouwbaarheidseisen aan de onderdelen ervan gesteld worden. Van het proces tot aan de elektriciteitsvoorziening zijn de betrouwbaarheidseisen aangegeven.

Onderstaande figuur geeft de configuratieanalyse van het proces 'Behandelen' aan:



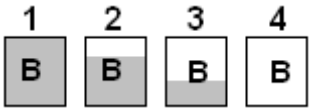
Figuur 6: Configuratieanalyse van het proces behandelen

Indien een proces gebruik maakt van bijvoorbeeld meerdere server/cliënt informatiesystemen, zullen de hoogste betrouwbaarheidseisen overgeërfd worden.

De betrouwbaarheidseisen zijn aan de hand van een figuur aangegeven:

Figuur 7: Betrouwbaarheidseisen

De inhoud van het blokje bepaalt de mate van de betrouwbaarheid. Hoe voller het blokje is, des te hoger de betrouwbaarheidseis. Deze manier van werken wordt verder uitgewerkt in de literatuur "*Informatiebeveiliging onder controle*".



1. Essentieel
2. Belangrijk
3. Wenselijk
4. Geen criterium

Met de configuratieanalyse kan direct gezien worden welke objecten aanwezig zijn en wat de betrouwbaarheidseis is. Voor de complete configuratieanalyse van alle processen verwijs ik u door naar bijlage VI.

De volgende paragraaf beschrijft het vaststellen van de externe eisen.

3.6 Externe eisen vaststellen

Om te bepalen aan welke eisen op het gebied van informatiebeveiliging de Rooyse Wissel dient te voldoen, is er onderzoek gedaan naar de geldende normen. Na overleg met het Hoofd I&A en met een beleidsmedewerker, is het internet geraadpleegd. Hier kwam al snel uit dat we gebruik gingen maken van de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging beschrijft de normen en maatregelen, die van belang zijn voor het realiseren van een afdoende niveau van informatiebeveiliging.
Een norm die gebaseerd is op deze Code voor Informatiebeveiliging, is de NEN7510. Deze norm is ontwikkeld voor de zorgsector. De reden hiervoor is dat er met name specifieke extra aandachtspunten zijn, zoals privacybescherming.

Aan de hand van deze NEN7510 norm, zijn de beveiligingseisen getoetst aan de werkelijke situatie binnen de Rooyse Wissel. In de volgende paragraaf wordt hier verder op ingegaan.

3.7 Checklist informatiebeveiliging (GAP-analyse)

Wat houdt een GAP-analyse precies in? De GAP is het verschil tussen de werkelijke situatie en wenselijke situatie (norm). Aan de hand van deze analyse wordt dit verschil zichtbaar en is ook duidelijk te zien op welke gebieden de Rooyse Wissel nog niet voldoet aan de norm.

Om de GAP in kaart te brengen, is er gebruik gemaakt van een checklist. Deze checklist bevat de beveiligingseisen die beschreven staan in de NEN7510 norm (informatiebeveiliging in de zorg). De Rooyse Wissel dient te voldoen aan deze beveiligingseisen.

Samen met de informatiebeveiligingsfunctionaris zijn de verschillende beveiligingseisen getoetst en geaccordeerd. Onduidelijkheden zijn aan de hand van de NEN7510 onderzocht om tot een passend antwoord te komen. Na de eerste versie is de checklist samen met de informatiebeveiligingsfunctionaris en het Hoofd I&A getoetst. Het resultaat is een eerste definitieve versie van de status van informatiebeveiliging volgens de NEN7510.

Onderstaande figuur geeft een voorbeeld van enkele beveiligingseisen op het gebied van fysieke beveiliging en beveiliging van de omgeving.

Checklist NEN7510, Informatiebeveiliging in de zorg		
Normhoofdstuk/ Vraag	**Ja / Nee / Gedeeltelijk**	**Opmerking**
9. Fysieke beveiliging en beveiliging van de omgeving		
1. Is er een “clean desk” en “clear screen” beleid ingesteld?	Ja	Betere toetsing op clean desk noodzakelijk
2. Zijn maatregelen getroffen om te voorkomen dat het personeel zonder toestemming eigendommen van de instelling meeneemt?	Ja	Uitvoer beleid aanwezig Moet extra onder de aandacht gebracht worden -> receptie

Bij iedere vraag kan met ‘ja’, ‘nee’ of ‘gedeeltelijk’ worden geantwoord. ‘Ja’ betekent dat de maatregel volledig volgens de norm aanwezig is, is ingevoerd en wordt nageleefd. ‘Nee’ betekent dat dit (nog) niet het geval is. ‘Gedeeltelijk’ kan inhouden dat de maatregel wellicht in opzet wel aanwezig is, maar nog niet wordt nageleefd of dat delen van de instelling zich wel houden aan deze norm, maar andere delen nog niet. In het veld van de opmerkingen kan een toelichting op het gegeven antwoord worden

opgenomen. Op deze manier ontstaat een checklist van mogelijke verbetermaatregelen op de plaatsen waar geen antwoord 'ja' kan worden gegeven.

Het gebruik van de checklist is eigenlijk tegenstrijdig met de methode van de risicoanalyse die gekozen is. In de afsluiting zal hier verder op in worden gegaan.

De checklist informatiebeveiliging zal niet worden bijgevoegd als bijlage wegens vertrouwelijke informatie.

Aan de hand van deze checklist en de risk assessment, die in de volgende paragraaf besproken wordt, zullen de relevante bedreigingen zichtbaar worden. Deze bedreigingen zullen uiteindelijk samen met de kwetsbaarheden verwerkt worden in de maatregelenanalyse.

3.8 Bedreigingenanalyse

De bedreigingenanalyse wordt gebruikt om de meeste relevante bedreigingen binnen de organisatie te herkennen en te voorzien van een zogenaamde risicowaarde. Om de risicowaarde van een bedreiging te bepalen, moet de kans en de impact van de bedreiging duidelijk zijn. Aan de hand van een risk assessment kan deze risicowaarde bepaald worden en zal zo duidelijk worden welke bedreigingen het hoogste scoren. De risk assessment is samen met de systeembeheerder ingevuld.

Onderstaand een voorbeeldschema met de bedreigingen met verschillende risicowaardes:

Nr.	Bedreiging	Kans	Impact	Risk value
1	Beveiligingsinbreuken gerelateerd aan het beveiligingsbeleid	Low	Medium	2
2	Beveiligingsinbreuken veroorzaakt door ontbreken van bewustzijn	High	High	9
3	Beveiligingsinbreuken veroorzaakt door ontbreken van een beveiligingsorganisatie -en coördinatie	Medium	Medium	4
4	Beveiligingsinbreuken veroorzaakt door onduidelijke verantwoordelijkheden	Medium	High	6
5	Beveiligingsinbreuken veroorzaakt door zwakten in de beveiliging	Low	High	3

De risicowaarde is op de volgende manier berekend:

	Impact		
Kans	High	Medium	Low
High	9	6	3
Medium	6	4	2
Low	3	2	1

De complete bedreigingenanalyse is bijgevoegd als bijlage VII.

3.9 Kwetsbaarheidsanalyse

Een kwetsbaarheidsanalyse heeft tot doel te bepalen welke bedreigingen relevant zijn voor de objecten van een informatiesysteem en hoe kwetsbaar deze objecten zijn voor deze bedreigingen. Tevens wordt de mate van beveiliging bepaald die de objecten voor goed functioneren nodig hebben.

De kwetsbaarheidsanalyse bestaat uit een tweetal stappen:

- Het bepalen van de mate waarin de objecten kwetsbaar zijn voor bedreigingen met betrekking tot de drie betrouwbaarheidseisen;
- Het bepalen van de mate van beveiliging die per object van het informatiesysteem nodig is.

Het resultaat is een overzicht met de objecten, de mogelijke bedreigingen en de mate van beveiliging die nodig is. Deze kwetsbaarheidsanalyse is samen met de informatiebeveiligingsfunctionaris ingevuld.

Onderstaande figuur laat de waarde van kwetsbaarheid zien bij een aantal verschillende objecten:

		B				**I**				**V**		
Type object	**Bedreiging**	Invloed van buiten	Storing apparatuur	Sabotage	Verlies van gegevens	Storing apparatuur	Fouten	Invoerfouten	Virus	Menselijke fouten	Diefstal	Manipulatie
Informatiesysteem	EPD	-	o	oo	ooo	o	ooo	ooo	o	ooo	oo	ooo
Computersysteem	Server	o	oo	o	o	oo	o	o	ooo	o	o	o
	Draagbare media	oo	oo	oo	ooo	o	oo	oo	ooo	ooo	ooo	ooo
Basisvoorziening	Elektriciteitsvoorziening	oo	ooo	oo	-	-	-	-	-	-	-	o

ooo = hoog, oo =gemiddeld, o = laag, - = n.v.t.

Aan de hand van de kwetsbaarheid van het object en het belang van het object, wordt het beveiligingsniveau bepaald. Dit beveiligingsniveau wordt op de volgende manier bepaald:

		Kwetsbaarheid van object voor bedreiging			
		ooo	oo	o	-
Betrouwbaarheidseis	Essentieel	H	G	L	N
	Belangrijk	G	L	N	N
(B, I, V)	Wenselijk	L	N	N	N
Voor object	Geen criterium	N	N	N	N

H = Hoog, G = Gemiddeld, L = Laag, N = Nihil

Om te bepalen op welk niveau de beveiliging moet liggen, zijn de afhankelijkheidsanalyse en kwetsbaarheidsanalyse in de volgende tabel samengevoegd per kwaliteitsaspect. Hierbij telt de hoogste score uit beide analyses. Onderstaande figuur een aantal objecten met het bijbehorende beveiligingsniveau:

		B			**I**			**V**		
		configuratie	kwetsbaarheid	beveiligingsniveau	configuratie	kwetsbaarheid	beveiligingsniveau	configuratie	kwetsbaarheid	beveiligingsniveau
Programmatuur	EPD	E	ooo	H	E	ooo	H	E	ooo	H
Computersysteem	Server	E	oo	G	E	ooo	H	E	o	L
	Draagbare media	W	ooo	L	E	ooo	H	E	ooo	H
Basisvoorziening	Elektriciteitsvoorziening	E	ooo	H	E	-	N	E	o	L

H = Hoog, G = Gemiddeld, L = Laag, N = Nihil

De grijze gebieden betreffen een gewenst beveiligingsniveau nihil. Hier zijn dus geen maatregelen nodig. De groene gebieden betreffen een laag beveiligingsniveau. Hier zijn dus slechts eenvoudige maatregelen nodig. De oranje en rode gebieden zijn de werkelijke aandachtsgebieden.

De volledige kwetsbaarheidsanalyse is toegevoegd als bijlage VIII.

3.10 Maatregelenanalyse

Een maatregelenanalyse heeft tot doel te bepalen welke (beveiligings)maatregelen nodig zijn om het te beschouwen informatiesysteem zodanig te beveiligen dat alle risico's, die nog overblijven, acceptabel zijn.

Het uitgangspunt van een maatregelenanalyse is een opsomming, waarin voor ieder object is aangegeven tegen welke bedreigingen het betreffende object beveiligd dient te worden en welk beveiligingsniveau daarbij nodig is. Tevens is een kolom toegevoegd om aan te geven of de maatregelen ingevoerd zijn of nog niet.

In dit hoofdstuk onderscheiden we de maatregelenanalyse aan de hand van:

- Kwetsbaarheidsanalyse
- GAP-analyse
- Bedreigingenanalyse / Risk assessment

Als eerste de maatregelenanalyse t. o. v. de kwetsbaarheidanalyse. Onderstaand een voorbeeld van enkele objecten met bijbehorend beveiligingsniveau en de maatregelen:

Type object	**Object**	**Bedreiging**	**Beveiligingsniveau**	**Maatregelen**	**Ingevoerd**
Programmatuur	EPD	Verlies van gegevens	Hoog (B)	- Authenticatie - Back-up van gegevens - Beveiligde omgeving	
		Fouten	Hoog (I)	- Uitwijk van applicatie	
		Invoerfouten	Hoog (I)	- Validatie van invoer - Controle door derde	
		Menselijke fouten	Hoog (V)	- Procedures opstellen - Disciplinaire acties formuleren	
		Manipulatie	Hoog (V)	- Authenticatie - Functiescheiding	
Computersysteem	Server	Storing apparatuur	Gemiddeld (B)	- Uitwijkmogelijkheid - Back-up	
		Storing apparatuur	Hoog (I)	- Uitwijkmogelijkheid - Back-up	
		Virus	Hoog (I)	- Back-up	
	Draagbare media	Verlies van gegevens	Laag (B)	- Truecrypt beveiliging	
		Virus	Hoog (I)	- Scannen bij invoer - Niet direct aan het netwerk	
		Manipulatie	Hoog (V)	- Truecrypt beveiligd - USB poorten authenticatie	
Basisvoorziening	Elektriciteitsvoorziening	Storing apparatuur	Hoog (B)	- Noodstroom voorziening	

Als tweede de maatregelenanalyse t. o. v. de GAP-analyse. Binnen deze maatregelenanalyse zijn alleen de eisen, die beoordeeld zijn met 'nee', meegenomen. Onderstaand enkele objecten met bijbehorende risico's, de risicostatus en de maatregelen:

Beveiligingseis	Risico	Risico status	Maatregelen	Ingevoerd
Zijn de verantwoordelijkheden voor informatiebeveiliging opgenomen in de functieomschrijving?	Onduidelijke verantwoordelijkheden op het gebied van informatiebeveiliging	Risiconeutraal	Awareness campagne informatiebeveiliging Opnemen in functieomschrijving	
Is een duidelijk beleid geformuleerd ten aanzien van het gebruik van elektronische communicatie?	Informatie naar verkeerd e-mailadres verzenden	Risicodragend	Procedures opstellen Validatie van e-mailadres	
Worden gebruikersautorisaties regelmatig gecontroleerd (bijvoorbeeld om de zes maanden)?	Onterechte autorisaties voor medewerkers Geen inzicht in autorisaties van medewerkers	Risiconeutraal	Periodieke autorisatie controle	

Als risicostatus kunnen verschillende statussen worden ingevuld. Onderstaand de betekenis van de verschillende statussen:

- Risicomijdend, een zo gering mogelijk risico ongeregeld te laten;
- Risiconeutraal, kosten voor beveiliging min of meer in evenwicht houden met de kosten die gemoeid zijn met schade;
- Risicodragend, meer risico accepteren dan men afdekt;

Als derde de maatregelenanalyse t. o. v. de bedreigingenanalyse / risk assessment. Dit onderdeel van de maatregelenanalyse, die meegenomen is als bijlage, laat de bedreigingen met een risk value van 6 of hoger zien. Deze bedreigingen hebben ofwel een kans of impact die met hoog beoordeeld is. Hierdoor is het van belang dat deze bedreigingen zo goed mogelijk opgevangen dienen te worden.

Onderstaand enkele objecten met bijbehorende NEN7510 hoofdstuk en maatregelen:

Bedreiging	Value 1-9	NEN7510 Hoofdstuk	Maatregelen	Opmerking	Ingevoerd
Beveiligingsinbreuken veroorzaakt door ontbreken van bewustzijn	9	5, 7, 8	Awareness campagne		
Beveiligingsinbreuken veroorzaakt door moedwillige actie en gemis aan disciplinaire actie	9	8, 15	Beleid opstellen Bedrijfscultuur verbeteren	Kans van slagen groot, kans dat medewerker uitvoert klein	
Fraude	9	8, 10	Beleid opstellen t.b.v. fraude	Kans van slagen groot, kans dat medewerker uitvoert klein	
Vrijgave van vertrouwelijke informatie	9	6, 7, 8, 9, 10, 12, 15	Vertrouwelijke informatie beveiligen Autorisatie voor beveiligde omgevingen Controle voor printen hardcopy	bv. afdrukken op verkeerde printer	

Voor de gehele maatregelenanalyse verwijs ik u naar bijlage IX.

4. Afsluiting

Is de informatiebeveiliging binnen F.P.C. de Rooyse Wissel voldoende op orde, om ongewenste schade te voorkomen? In dit hoofdstuk wordt antwoord gegeven op deze vraagstelling en worden de belangrijkste conclusies getrokken. Daarnaast wordt op basis van de conclusies aanbevelingen gedaan voor de toekomst.

4.1 Conclusie

De vraagstelling uit paragraaf 1.3 is door de uitkomst van dit project positief beantwoord. De informatiebeveiliging binnen de Rooyse Wissel is voldoende op orde om ongewenste schade te voorkomen. In de toekomst zal het echter van belang zijn om van voldoende op orde naar goed tot uitstekend op orde te gaan.

Het project is vooral gericht op het kwaliteitsaspect vertrouwelijkheid, echter is er in enkele conclusies ook rekening gehouden met de integriteit en beschikbaarheid van informatie. Hier is ook rekening mee gehouden, omdat dit in het kader van informatiebeveiliging binnen de huidige situatie van belang is.

Het volgende is uit de onderzoeken en aan de hand van dagelijkse gesprekken op de afdelingen geconcludeerd:

1. De awareness van de medewerkers op het gebied van informatiebeveiliging moet verbeterd worden.

2. Verschillende risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie aan kunnen tasten, dienen gedekt te worden.
    a. Invoerfouten
    b. Applicatie fouten
    c. Menselijke fouten
    d. Draagbare media

3. Taken en verantwoordelijkheden omtrent informatiebeveiliging zijn niet bekend bij medewerkers.

4. Procedures en beleid over werkwijze

4.2 Aanbevelingen

Aan de hand van de getrokken conclusies uit de vorige paragraaf zijn een aantal aanbevelingen opgesteld.

1. Om de bewustwording van de medewerkers op het gebied van informatiebeveiliging te verbeteren is het van belang om een awareness campagne te houden. Dit is de taak van de informatiebeveiligingsfunctionaris. Deze campagne bestaat uit een aantal presentaties op de verschillende afdelingen. Op deze manier worden de medewerkers betrokken bij informatiebeveiliging, omdat elke afdeling met vertrouwelijke informatie werkt en moet weten hoe hiermee omgegaan dient te worden.

2. Uit de verschillende analyses komen we risico's tegen die gedekt of uitgeschakeld kunnen worden:
    a. Op het gebied van invoerfouten, kunnen bijvoorbeeld validaties en controles door anderen worden uitgevoerd. Validaties inbouwen in de bestaande informatiesystemen zal het beste werken. In combinatie met een tweede en eventueel een derde controle zal dit risico zo goed als uitgeschakeld zijn.
    b. Op het gebied van applicatie fouten is het van belang dat de werkzaamheden hun doorgang kunnen vinden. Door gebruik te maken van een uitwijkmogelijkheid is dit te realiseren. Werkzaamheden zullen niet lijden onder fouten die zich in applicaties bevinden, waardoor de beschikbaarheid, integriteit en vertrouwelijkheid van de informatie omlaag gaat. De uitwijkmogelijkheid zal op de locatie OGH in Zetten moeten worden opgezet. Deze locatie dient dan ook te voldoen aan de eisen uit de NEN7510.
    c. Op het gebied van menselijke fouten zullen er standaard werkwijzen beschreven moeten worden. Ook is het van belang dat medewerkers ervan bewust zijn dat controles op werkzaamheden belangrijk zijn. Menselijke fouten voorkomen is beter dan genezen. Disciplinaire acties dienen ook beschreven worden bij opzettelijke fouten, waardoor de integriteit en vertrouwelijkheid van informatie beschadigd raken.
    d. Op het gebied van gegevensopslag op draagbare media zijn grote vraagtekens. Het is onduidelijk voor medewerkers, wie en hoe gebruik gemaakt dient te worden met USB-sticks waarop vertrouwelijke informatie zich bevindt. Ongeoorloofde toegang tot vertrouwelijke informatie is op deze manier aanzienlijk groot. Het is van groot belang dat er een beleid en procedures worden opgesteld om de werkwijze en authenticatie te beschrijven. Enkele vragen die van belang zijn bij correct USB gebruik:
        - Zetten we de USB poorten voor elk werkstation open/dicht?
        - Koppelen we USB gebruik aan functie?
        - Koppelen we USB gebruik aan bepaalde werkstations? (leidinggevende)
        - Welke USB sticks mogen wel en welke juist niet gebruikt worden?
        - Hoe zullen patiënten gebruik gaan maken van USB sticks? (huiswerk)

3. Medewerkers dienen op de hoogte te zijn van taken en verantwoordelijkheden omtrent informatiebeveiliging. Om dit te realiseren is er de mogelijkheid om deze taken en verantwoordelijkheden op te nemen in de functieomschrijving. Ook is het van belang om eventueel jaarlijks de kennis over deze taken en verantwoordelijkheden te toetsen bij verschillende medewerkers.

4. Het is van groot belang dat medewerkers weten hoe ze om moeten gaan met vertrouwelijke informatie. Vaak wordt er gedacht dat hun manier van werken de beste en veiligste is. De procedures omtrent uitwisselen, muteren, valideren en kopiëren van gegevens moeten goed beschreven staan en centraal voor iedereen beschikbaar zijn. Het is dus noodzakelijk dat deze documenten geschreven worden. Hierdoor zullen medewerkers elk op dezelfde manier werken en deze manier van werken zorgt voor een zo hoog mogelijk informatiebeveiligingsgehalte.

4.3 Methode

Voordat het project daadwerkelijk van start is gegaan, is er door de stagiair een vooronderzoek gedaan naar de meest geschikte methodes. Deze methodes zijn beschreven in dit rapport. Is het project nou daadwerkelijk uitgevoerd volgens deze methodes?

Het antwoord op deze vraag is gedeeltelijk. De methode die gekozen is om de risicoanalyse uit te voeren is de kwalitatieve risicoanalyse. Binnen deze methode zijn de risico's, bedreigingen en maatregelen beschreven. Geen checklists, maar een geheel op maat gemaakt onderzoek.
Tijdens het project is echter wel gebruik gemaakt van een checklist. Deze checklist is gebruikt om te toetsen in hoeverre de Rooyse Wissel voldoet aan de eisen binnen de NEN7510. Het toetsen aan de NEN7510 is in principe het afvinken van eisen waar al aan voldaan wordt en markeren van eisen waar (nog) niet aan voldaan wordt. Om dit te realiseren is er een checklist gemaakt met de beveiligingseisen uit de NEN7510, om het toetsen van de werkelijke situatie te vereenvoudigen.

Tevens is er ook gebruik gemaakt van een quickscan. De quickscan is weer een andere methode om de risicoanalyse uit te voeren. Deze quickscan is uitgevoerd op de locatie OGH in Zetten. OGH is sinds kort een samenwerkingsverband aangegaan met de Rooyse Wissel. Hierdoor is het van belang dat de beveiligingseisen van beide locaties in evenwicht zijn. Doordat de locaties voor elkaar de uitwijkmogelijkheid zullen worden, dient de beveiliging bij OGH evenredig te zijn aan de beveiliging van de Rooyse Wissel. Samen met de systeembeheerder van OGH is een quickscan uitgevoerd en is nu in kaart gebracht in hoeverre OGH voldoet aan de norm.

Op het gebied van de BSP-methode die beschreven is in dit rapport, zijn geen aanpassingen gedaan. Het informatiekruis is geheel via de methode beschreven.

De A, B & K-analyse is tevens uitgevoerd, zoals deze beschreven is in dit rapport en volgens de literatuur *"Informatiebeveiliging onder controle".*

Het projectactiviteitenschema laat precies zien welke activiteiten zijn uitgevoerd. Deze resultaten zijn (deels) opgenomen in de bijlage.

Gedurende het project zijn dus aanpassingen ingevoerd omtrent de risicoanalyse methode. De methode die daadwerkelijk is toegepast, is een combinatie van de verschillende methodes om het gewenste resultaat te bereiken. Er is dus niet blindelings uitgegaan van een methode, maar er is een methode gekozen als referentie waar naar eigen inzicht en ervaringen verbeteringen in zijn toegepast.

5. Literatuuropgave

Dit hoofdstuk geeft een bronvermelding, opgesplitst in literatuur en websites. Deze hebben bijgedragen aan het succesvol afronden van de tussenproducten en het eindproduct.

5.1 Literatuur

De volgende literatuur is ter naslag gebruikt:

NEN-7510:2004, Medische informatica - Informatiebeveiliging in de zorg – Algemeen

Handreiking van NOREA (2003)

Fijneman, R. Lindgreen, E.R. Ho, K.H., *IT-auditing en de praktijk*, Sdu Uitgevers BV (2006)
ISBN: 90 395 2468 8

Overbeek, P. Lindgreen, E.R. Spruit, M., *Informatiebeveiliging onder controle,* Pearson Education Benelux BV (2006)
ISBN: 978 90 430 0692 7

Grit, R., *Projectmanagement*, Houten (2005)
ISBN: 978 90 013 4703 1

5.2 Websites

Onderstaande websites zijn gebruikt voor informatie:

http://www.derooysewissel.nl
Website van F.P.C. de Rooyse Wissel

http://www.fontys.nl
Website van Fontys Hogescholen

http://www.xs4all.nl/~rvy/ib-ak-analyse.html
A, B & K-analyse

https://lab.cs.ru.nl/BusinessRules/Information_security_in_the_medical_domain
Information security in the medical domain

6. Bijlagen

I *plan van aanpak*
II *identificatie informatiesystemen*
III *beschrijving processen*
IV *informatiekruis*
V *afhankelijkheidsanalyse*
VI *configuratieanalyse*
VII *bedreigingenanalyse*
VIII *kwetsbaarheidsanalyse*
IX *maatregelenanalyse*
X *IT-audit rapport*
XI *adviesrapport*
XII *persoonlijke evaluatie*