

HOGESCHOOL
UTRECHT
MASTER OF INFORMATICS



MASTER'S THESIS

Continuïteit van informatievoorziening bij kritische zorgprocessen

Onderzoek naar een beoordelingsinstrument continuïteitsbeheer

Author:

Peter Vermeulen

Date:

July, 2008

Hogeschool Utrecht
Faculty Science and Engineering
P.O. box 182
3500 AD UTRECHT
The Netherlands

Continuïteit van informatievoorziening bij kritische zorgprocessen

Onderzoek naar een beoordelingsinstrument continuïteitsbeheer

Thesis Master of Informatics

Opdrachtgever: Kees de Jong, hoofd patiëntenzorg en koppelingen, Directie Informatie
Technologie UMC Utrecht

Thesisbegeleider: Pascal Ravesteijn, Hogeschool Utrecht

Auteur: Peter Vermeulen,

Email: p.w.vermeulen@umcutrecht.nl

Datum: 27 juli 2008

Versie: 1.0

Voorwoord

Deze Thesis is onderdeel van de afronding van de studie Master of Informatics aan de Hogeschool Utrecht. In een periode waarin de vaste structuur van colleges en tentamens wegvalt, sta je als student in het laatste half jaar nadrukkelijk zelf aan het roer. Niet de makkelijkste, wel een leerzame en boeiende periode.

Hulp is dan van harte welkom. Je kunt jezelf helpen door een onderwerp te kiezen, welke je écht de moeite waard vindt. Voor mij is continuïteitsbeheer zo'n onderwerp. Natuurlijk is het als 'automatiseerder' mooi om te zien als zorgverleners geholpen zijn met geautomatiseerde informatieverwerking. Het maakt je tegelijkertijd des te meer bewust van je verantwoordelijkheid om mee te denken bij de consequenties van afhankelijkheid van ICT.

Ik ben goed ondersteund door de collega's in het UMC Utrecht en de twee andere UMC's. Ik ga hier niet alle namen noemen, simpelweg omdat het er te veel zijn en ik deze mensen heb toegezegd de informatie anoniem te verwerken. Het zijn deze mensen met veelal drukke agenda's en uitpuilende mailboxen die, zonder uitzondering, tijd wisten te maken om écht betrokken in dit onderzoek met me mee te denken.

Wel met name noem ik Kees de Jong, formeel opdrachtgever van dit onderzoek, maar vooral ook altijd aanspreekbaar als klankbord op het werk. Ook Hans Maring, security officer in het UMC Utrecht, heeft me erg goed geholpen. Het is waardevol te kunnen 'sparren' met iemand die uitgebreide kennis van het onderwerp en ervaring in de ziekenhuisorganisatie heeft.

Vanuit de Hogeschool Utrecht heeft mijn thesis begeleider, Pascal Ravesteijn, mij prima bijgestaan. Enerzijds door deskundig en goed gefundeerd feedback te geven op alle tussenproducten. Anderzijds door op een prettige en betrokken manier mee te denken en steeds weer snel te reageren op mijn vragen. Maar misschien nog wel het meest doordat we samen de balans hebben gevonden tussen het leren doen van onderzoek én het werken aan een praktisch toepasbaar hulpmiddel voor de organisatie. Zo is volgens mij het concept van de *Professional Master* bedoeld.

Toch zou het allemaal niet gelukt zijn als ik niet de enorme steun van het thuisfront had gehad. Zo'n studie doe je echt met zijn allen. Bertine, die voortdurend met me heeft meegedacht, en heel veel zorgen buiten de studie om heeft gedragen. En de jongens, Bram, Luuk en Thomas, die ook maar wát geduld met hun vader hebben gehad als hij zich weer eens afzonderde achter de pc op zolder. Hierdoor kan ik met veel plezier en trots op deze periode terugkijken.

Peter Vermeulen

Juli 2008

Samenvatting

In de gezondheidszorg is sprake van een toenemende afhankelijkheid van geautomatiseerde informatievoorziening in de primaire bedrijfsprocessen. Binnen de patiëntenzorg is de beschikbaarheid van informatie essentieel voor patiëntveiligheid, maar ook voor aspecten als efficiëntie en kwaliteit van zorg. Voor een ziekenhuis is het dan ook van belang om inzicht te hebben in hoe het continuïteitsbeheer rondom deze informatievoorziening is geregeld.

In dit onderzoek is een antwoord gezocht naar de vraag:

“Hoe kan een ziekenhuis bij implementatieprojecten van zorgkritische ICT beoordelen of voldoende maatregelen zijn genomen voor het vaststellen en verminderen van risico's, beperken van gevolgen van incidenten en tijdig hervatten van werkzaamheden in het geval van uitval van deze systemen?”

Om tot een antwoord te komen is het volgende proces doorlopen. Allereerst een literatuurstudie waarin belangrijke aspecten rondom Business Continuity Management en informatievoorziening in de gezondheidszorg in kaart zijn gebracht. Het gaat hierbij allereerst om de fasen welke in het proces continuïteitsbeheer van belang zijn; die van analyse, maatregelen, evaluatie, testen en onderhoud. Daarnaast ook regelgeving en standaarden op het gebied van informatiebeveiliging en continuïteitsbeheer. Voor de Nederlandse gezondheidszorg is NEN7510 belangrijk. Het is de norm die ook gevolgd moet gaan worden voor uitwisseling van patiëntgegevens in het kader van de landelijke EPD ontwikkelingen.

De gevonden criteria zijn in interviews voorgelegd aan belanghebbenden binnen het UMC Utrecht. Hierbij is tot onderstaande definitieve lijst van criteria gekomen waaraan bestaande beoordelingsinstrumenten voor BCM getoetst kunnen worden.

Inhoudelijke aspecten

- Risicoanalyse
- Business Impact Analyse
- Maatregelen
- Evaluatie
- Organisatie

Kwaliteitsaspecten

- Efficiëntie
- Objectief
- Normerend
- Valide
- Voldoen aan regelgeving

Scope van meetinstrument

- Meten op niveau bedrijfsproces (detailniveau)
- Meten op proces patiëntenzorg (domein)
- Meten op informatievoorziening

In het onderzoek zijn een vijftal bestaande beoordelingsinstrumenten voor BCM nader bekeken.

- Monitor Informatiebeveiliging 2.008
- NEN7510 checklist continuïteitsplanning
- Business Continuity Maturity Model
- BCI PAS56 Audit Workbook v2.0
- Checklist Code voor informatiebeveiliging

Toetsing aan de gedefinieerde criteria laat zien dat één van de instrumenten, de checklist Code voor Informatiebeveiliging, als beste instrument beoordeeld wordt, maar dat andere instrumenten ook hun specifieke kwaliteiten kennen.

De volgende stap in het onderzoek is het combineren van de verschillende kwaliteiten in een nieuwe beoordelinginstrument voor continuïteitsbeheer. Dit instrument is voorgelegd aan stakeholders in het UMC Utrecht en twee andere vergelijkbare ziekenhuizen. Uit de gehouden enquête komen verschillende suggesties ter verbetering naar voren. In z'n algemeenheid voldoet het instrument op aspecten van gebruik en het verschaffen van inzicht in de status van continuïteitsbeheer. Een casestudy, waarbij het instrument gebruikt is voor het beoordelen van een bestaand bedrijfsproces in het UMC Utrecht, valideert de bruikbaarheid.

Geconcludeerd kan worden dat het nieuwe beoordelingsinstrument een goed hulpmiddel is bij het geven van inzicht in continuïteitsbeheer rondom zorgkritische ICT-toepassingen. Aandacht is nog nodig voor vragen rondom implementatie van het instrument. Wie moet het gaan invullen, hoe past het in een breder beleid op het gebied van Business Continuity Management? Ook kan als vervolg van dit onderzoek het beoordelingsinstrument nog verder verbeterd worden, zowel waar het gaat om inhoudelijke aanscherping als in de presentatievorm.

Inhoudsopgave

Voorwoord	iii
Samenvatting.....	v
Inhoudsopgave	1
Lijst met afbeeldingen.....	2
Lijst met tabellen.....	2
1. Inleiding.....	5
1.1. Belang van Business Continuity Management	5
1.2. Concreet aan de slag met BCM	7
1.3. Onderzoeksvraag	7
1.4. Afbakening	8
1.5. Structuur van het onderzoek	8
1.6. Onderzoekstechnieken	9
1.7. De opdrachtgever	11
2. Business Continuity Management	13
2.1. Begripsdefinitie.....	13
2.2. Informatiebeveiliging en continuïteitsbeheer	15
2.3. Inhoudelijke aspecten BCM	16
2.4. Regelgeving, normen	19
2.5. BCM en gezondheidszorg	22
2.6. Stakeholders	24
2.7. Samenvatting	24
3. Beoordelingsinstrument voor BCM	27
3.1. Een beoordelingsinstrument	27
3.2. Bestaande beoordelingsinstrumenten	28
3.3. Concept criteria beoordelingsinstrument	34
3.4. Samenvatting	36
4. Interviews toetsing criteria beoordelingsinstrument.....	39
4.1. Opzet interviews.....	39
4.2. Resultaten	40
4.3. Definitieve criteria beoordelingsinstrument	43
4.4. Samenvatting	44
5. Beoordeling van de referentie-instrumenten	47
5.1. Methode beoordeling referentie-instrument	47
5.2. Resultaat beoordeling referentie-instrumenten.....	49
5.3. Samenvatting	52
6. Een nieuw beoordelingsinstrument.....	53
6.1. Methode van ontwikkeling.....	53
6.2. Opzet nieuw beoordelingsinstrument.....	54

6.3. Samenvatting	59
7. Validatie beoordelingsinstrument.....	61
7.1. Aanpak enquête	61
7.2. Resultaten enquête	62
7.3. Aanpak casestudy	67
7.4. Resultaten casestudy	68
7.5. Samenvatting	69
8. Conclusies en verder onderzoek	71
8.1. Antwoord op de onderzoeksvragen	71
8.2. Vervolgstappen en aanbevelingen.....	73
9. Bronnen	75
Bijlage 1: Planning onderzoek	79
Bijlage 2: Interview Toetsing aspecten BCM en criteria Meetinstrument	80
Bijlage 3: Schermafdrukken nieuw beoordelingsinstrument	86
Bijlage 4: Enquête validatie beoordelingsinstrument	93
Bijlage 5: Interviewvragen casestudy	95

Lijst met afbeeldingen

Figuur 1 IT-prioriteiten CIO's HIMMS 2008 (vertaald) [4].....	6
Figuur 2 Afbakening onderzoek	8
Figuur 3. Onderzoeksstructuur en hoofdstukindeling.....	9
Figuur 4 Beschikbaarheid informatie voor kritische processen.....	16
Figuur 5 Business Continuity Management Lifecycle [21]	17
Figuur 6 Diagram Monitor Informatiebeveiliging.....	30
Figuur 7 PAS 56 - Current State Assessment [41].....	32
Figuur 8 BCMM standard reference chart [45]	33
Figuur 9 Maturity Model for BCM - Naomi Smit [15]	34
Figuur 10 Scoreberekening BCI PAS56 Audit Workbook	56
Figuur 11 Scoreberekening nieuw beoordelingsinstrument	57
Figuur 12 Voorbeeld van een radardiagram [52]	58
Figuur 13 Radardiagram nieuw beoordelingsinstrument	59
Figuur 14 Planning Onderzoek Gannt Chart.....	79

Lijst met tabellen

Tabel 1 Concept criteria beoordelingsinstrument.....	35
Tabel 2 Definitieve criteria beoordelingsinstrument	43
Tabel 3 Scoringscriteria beoordelingsinstrumenten	47
Tabel 4 Beoordeling referentie-instrumenten	50
Tabel 5 Algemene gegevens.....	54

Tabel 6 Antwoordmogelijkheden beoordelingsinstrument	56
Tabel 7 Vragen met wegingsfactor 0,5.....	57
Tabel 8 Respondenten enquête	61
Tabel 9 Enquête - Inhoudelijke opmerkingen per vraag	65

1. Inleiding

De afgelopen jaren heeft ICT-ondersteuning in de gezondheidszorg een enorme groei doorgemaakt. In ziekenhuizen zijn zorggerelateerde gegevens zoals verslagen, brieven, röntgenfoto's, laboratoriumuitslagen, administratieve en logistieke informatie digitaal opgeslagen. De arts speelt hierin een actieve rol. Niet alleen voor naslag van deze informatie, maar in toenemende mate ook bij elektronische vastlegging van gegevens. Het gaat hierbij om dossiervoering en bijvoorbeeld elektronische orders zoals voorschrijven van medicatie en aanvragen van onderzoeken. Aan het werken met een elektronisch patiëntendossier (EPD) worden diverse voordelen toegeschreven. Denk aan patiëntveiligheid, kwaliteit van zorg en efficiency. [1] Vergelijkbare (potentiële) voordelen worden gevonden in verschillende wetenschappelijke studies. [2]

Echter het werken met ICT kent ook risico's. In 2004 heeft de Inspectie voor de gezondheidszorg onderzoek gedaan naar ICT in ziekenhuizen. In het rapport concludeert de inspectie dat zorgondersteunende ICT-toepassingen geen achterstand meer hebben ten opzichte van administratieve ICT-toepassingen. Vergeleken met de administratieve systemen zijn echter bij zorgondersteunende ICT de risico's rondom patiëntveiligheid veel groter. De inspectie uit in het onderzoek dan ook zijn zorgen over deze risico's. Het gaat hierbij om beveiliging, maar ook om mogelijke uitval van kritische systemen.

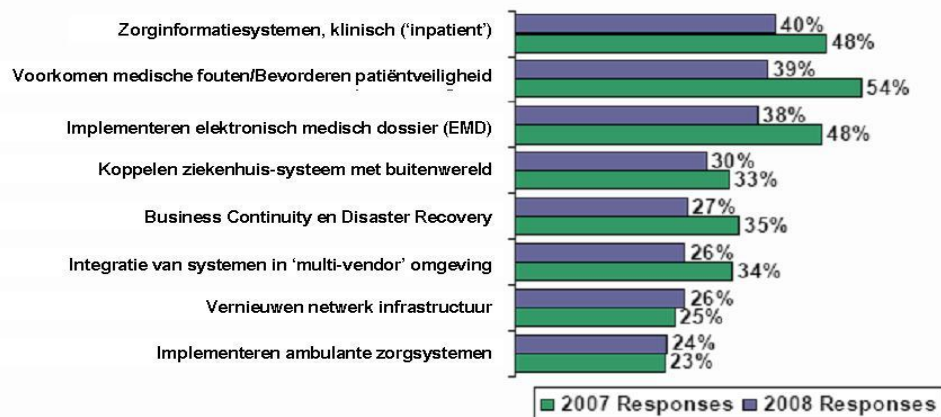
“Ziekenhuizen schenken op dit moment nog onvoldoende aandacht aan de risico's die de toepassing van ICT met zich meebrengt. De patiënt loopt hierdoor de kans op gevaar. Dat gevaar valt nu nog mee vanwege de beperkte toepassing van ICT, maar omdat door de bijna overal in gang gezette introductie van het elektronisch patiëntendossier binnen korte tijd de toepassing van ICT enorm zal zijn toegenomen, wordt dat gevaar aanzienlijk groter. In het onderzoek zijn geen duidelijke verschillen tussen de grotere en kleinere ziekenhuizen waargenomen.” [3]

1.1. Belang van Business Continuity Management

Ziekenhuizen onderkennen het belang van continuïteit in de informatievoorziening. De toonaangevende internationale organisatie voor 'healthcare information management systems society' (HIMMS), doet jaarlijks onderzoek onder Healthcare CIO's. In 2008 noemde 27% 'Business Continuity and Disaster Recovery' als huidige IT prioriteit. [4] Figuur 1 maakt duidelijk welke prioriteiten deze CIO's benoemen.

Huidige IT prioriteiten (komende 12 maanden)

(Resultaten 2008 tov 2007)



Figuur 1 IT-prioriteiten CIO's HIMMS 2008 (vertaald) [4]

In Nederland houdt het nationale normalisatie-instituut (NEN) zich bezig met een norm voor Informatiebeveiliging in de zorg. Continuïteitsbeheer maakt deel uit van deze 'NEN 7510'.

"Het proces van continuïteitsbeheer

Er moet een proces van continuïteitsbeheer worden geïmplementeerd om de verstoring als gevolg van calamiteiten en beveiligingsincidenten tot een aanvaardbaar niveau te beperken, door een combinatie van preventieve en herstelmaatregelen. Het continuïteitsbeheer moet maatregelen bevatten voor het vaststellen en verminderen van risico's, het beperken van de gevolgen van incidenten die schade toebrengen en het tijdig hervatten van essentiële werkzaamheden."[5]

Om aan te kunnen sluiten op het landelijk Elektronisch Patiënten Dossier moeten ziekenhuizen in de nabije toekomst voldoen aan de NEN 7510. Het landelijk EPD maakt het mogelijk om gegevens tussen verschillende zorgaanbieders uit te wisselen. Dit moet bijdragen aan een efficiëntere en veilige patiëntenzorg.

Regelgeving is niet de enige reden om Business Continuity Management (BCM) in het ziekenhuis in te voeren. Leegwater noemt in zijn artikel over BCM in de zorg een aantal andere factoren die hierbij een rol spelen [6]:

- hogere kwaliteitseisen
- toename interne en externe risico's (bijv. terreurdreiging)
- patiëntveiligheid
- imagoschade als dienstverlening voor langere tijd wordt onderbroken

1.2. Concreet aan de slag met BCM

Om continuïteitsbeheer rondom informatievoorziening in het ziekenhuis adequaat in te voeren is aandacht van verschillende stakeholders nodig. Het is een holistisch proces welke niet uitsluitend vanuit een ICT of juist een 'business'- perspectief bekeken kan worden. Samenwerking tussen de proceseigenaren in de zorg en vertegenwoordigers van ICT en facilitaire zaken is hierbij essentieel. [6] Daarbij is het belangrijk om vooraf vast te stellen wie nu eigenlijk 'eigenaar' van de verschillende zorgprocessen is. Een punt van aandacht is dat in praktijk niet altijd duidelijk is bij wie deze rol belegd is.

Een beoordelingsinstrument voor BCM kan helpen bij het nemen van de juiste maatregelen. Dit instrument zal, op basis van inschatting van risico's, kunnen blootleggen op welke aspecten er (on)voldoende aandacht is voor BCM. In dit onderzoek wordt gezocht naar een dergelijk instrument en getoetst of deze bruikbaar is bij het beoordelen van implementaties van zorgkritische ICT.

Voor het UMC Utrecht is dit onderzoek belangrijk. Met de toenemende afhankelijkheid van ICT wordt ook veel belang gehecht aan beschikbaarheid van de informatievoorziening. In het ICT-beleidsplan voor de periode 2006 tot 2010 wordt NEN 7510 als één van de uitgangspunten genomen bij inrichting van informatiebeveiliging. [7] Recente incidenten in andere ziekenhuizen, zoals de brand in een operatiecomplex, maken duidelijk dat BCM bittere noodzaak is. Het UMC Utrecht wil hiermee concreet aan de slag. Het formuleren van algemeen beleid hierover is niet voldoende. Juist een praktisch beoordelingsinstrument zal niet alleen het BCM proces kunnen ondersteunen, maar ook bijdragen aan een breder bewustzijn rondom dit thema.

1.3. Onderzoeksvraag

In dit onderzoek zal een antwoord gezocht worden op de vraag

“Hoe kan een ziekenhuis bij implementatieprojecten van zorgkritische ICT beoordelen of voldoende maatregelen zijn genomen voor het vaststellen en verminderen van risico's, beperken van gevolgen van incidenten en tijdig hervatten van werkzaamheden in het geval van uitval van deze systemen?”

Om deze onderzoeksvraag te kunnen beantwoorden is antwoord nodig op de volgende deelvragen

- 1) *Welke aspecten zijn van belang in BCM rondom ICT, essentieel voor uitvoering van directe patiëntenzorg?*
- 2) *Welke instrumenten zijn beschikbaar voor het beoordelen van BCM?*
- 3) *Aan welke criteria dient een beoordelingsinstrument voor BCM te voldoen?*

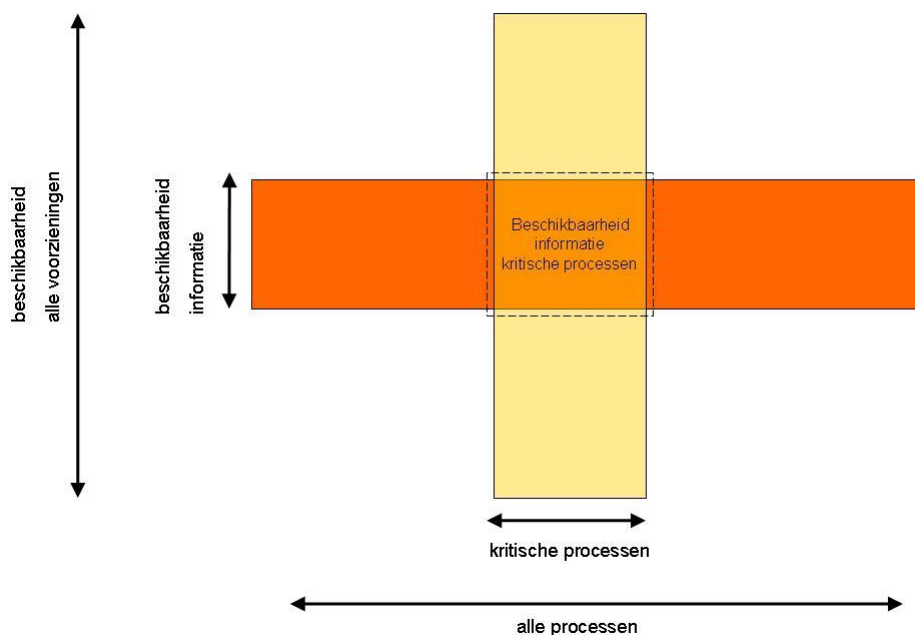
- 4) *Welke van de gevonden beoordelingsinstrumenten is het meest geschikt als referentie instrument?*
- 5) *Zijn er aanpassingen nodig in het referentie instrument om te voldoen aan de gestelde criteria?*

Als het antwoord op vraag 5 bevestigend is:

- 6) *Welke aanpassingen zijn nodig om het referentie instrument te laten voldoen aan de gestelde criteria?*

1.4. Afbakening

Bij Business Continuity Management gaat het om een holistisch proces waar verschillende soorten van bedreiging en verstoring van kritische bedrijfsprocessen aandacht hebben. Dit onderzoek beperkt zich tot beschikbaarheid van informatievoorziening voor deze kritische bedrijfsprocessen. Figuur 2 toont deze afbakening. Hoofdstuk 2 zal onderwerpen als Business Continuity Management en beschikbaarheid van informatie verder uitdiepen.

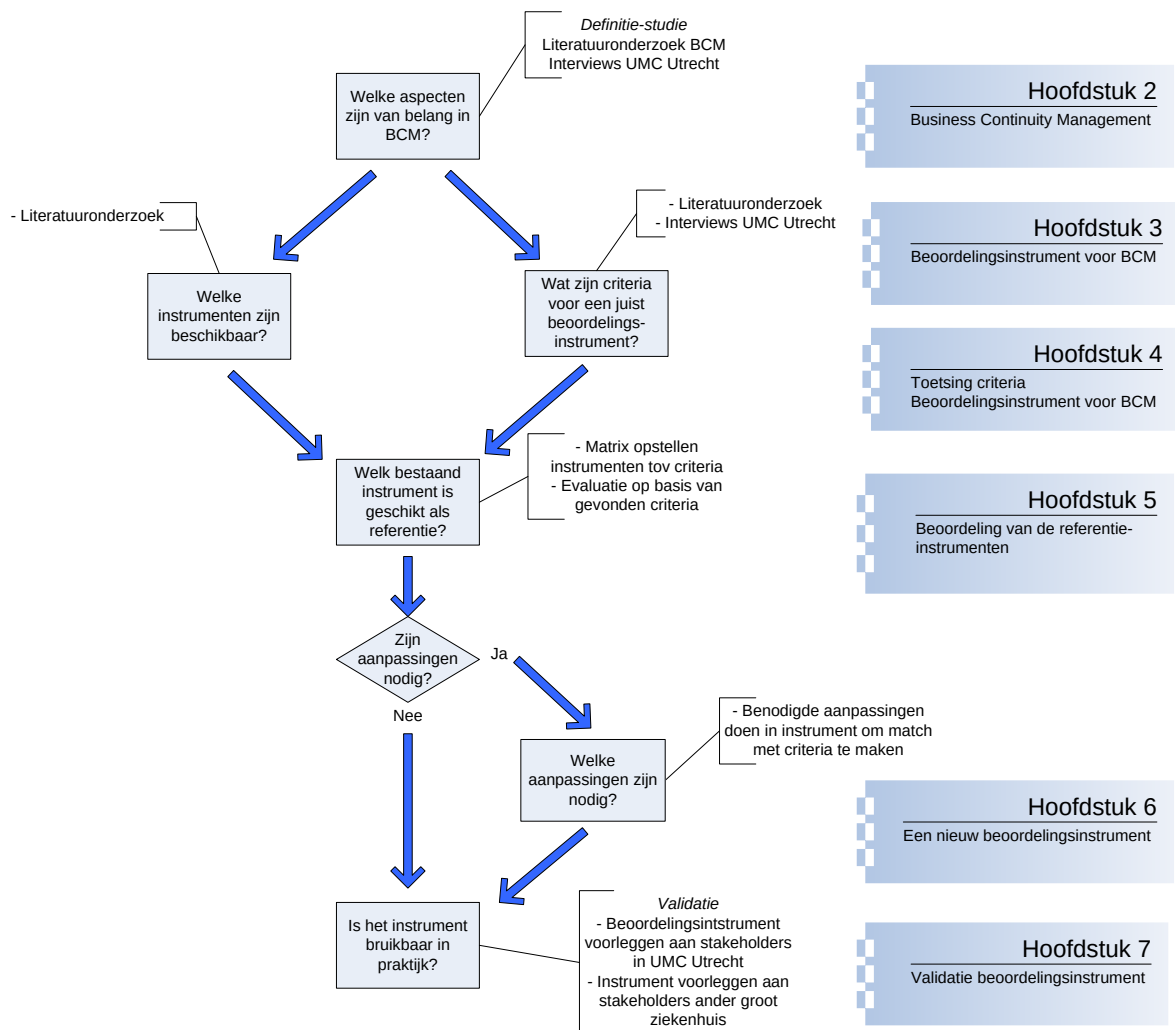


Figuur 2 Afbakening onderzoek

1.5. Structuur van het onderzoek

Om de onderzoeksvragen te kunnen beantwoorden zullen een aantal stappen doorlopen dienen te worden. De structuur van het onderzoek is grafisch weergegeven in figuur 3. Hierbij zijn bij de verschillende stappen ook de corresponderende hoofdstukken in het onderzoeksverslag

weergegeven. In bijlage 1 is de planning in tijd van de verschillende fasen van het onderzoek opgenomen.



Figuur 3. Onderzoeksstructuur en hoofdstukindeling

1.6. Onderzoekstechnieken

In dit onderzoek is gebruik gemaakt van verschillende onderzoekstechnieken, welke hieronder worden toegelicht.

1.6.1. Literatuuronderzoek

Door literatuuronderzoek zijn belangrijke aandachtsgebieden en stakeholders in BCM voor zorgkritische ICT in kaart gebracht. Ook is in de literatuur gezocht naar criteria waaraan een beoordelingsinstrument zal moeten voldoen. Bovendien is, vanuit de literatuur, een overzicht van bestaande beoordelingsinstrumenten gevormd.

1.6.2. Interviews

In gesprekken met belangrijke stakeholders in het UMC Utrecht zijn de in de literatuur gevonden aspecten en criteria voorgelegd, getoetst op volledigheid en te geven prioriteit. Er is hierbij gekozen voor de vorm van het 'gedeeltelijk gestructureerde interview'. Dit interview bestaat voor een deel uit gesloten vragen met een vaste formulering, die in een vaste volgorde worden gesteld. Hiernaast is de ruimte voor een aantal open vragen. [8] Deze vorm van interview biedt gelegenheid om naast de aspecten die door de onderzoeker zijn ingebracht, ook op nieuwe gezichtspunten, afkomstig van de geïnterviewde in te gaan.

1.6.3. Enquête

Het uiteindelijke beoordelingsinstrument is in de vorm van een enquête voorgelegd aan belangrijke stakeholders in het UMC Utrecht. De enquête is opgebouwd uit een korte toelichting bij het onderzoek en zeven open vragen. De laatste vraag geeft de mogelijkheid voor het plaatsen van overige opmerkingen en suggesties.

Deze enquête is ook gestuurd aan functionarissen in twee andere ziekenhuizen. Beide universitair medisch centra zijn in omvang vergelijkbaar met het UMC Utrecht. Het ene ziekenhuis kenmerkt zich door de afgelopen jaren een proactieve rol te spelen in het formuleren van beleid op het gebied van continuïteitsbeheer. Het andere ziekenhuis is op het gebied van keuzes in ICT en informatievoorziening zeer vergelijkbaar met het UMC Utrecht. Door deze andere ziekenhuizen te betrekken in het onderzoek kon bepaald worden of het instrument ook bruikbaar zou kunnen zijn buiten het UMC Utrecht. Gezien de toetsing bij een beperkte groep buiten het UMC Utrecht kan slechts met voorzichtigheid worden gesteld worden dat de resultaten van het onderzoek generaliseerbaar zijn voor andere ziekenhuizen.

De eerste enquêtes zijn in de vorm van een interview gedaan. Saunders beschrijft dit als een vorm van 'pilot testing' waarmee bepaald kan worden of de vraagstelling begrepen wordt en daarmee tot zinnige antwoorden zal leiden. [9]

1.6.4. Casestudie

Om de bruikbaarheid van het beoordelingsinstrument te toetsen is deze ook eenmalig voor een bestaand bedrijfsproces in het UMC Utrecht ingevuld. In deze casestudy is op een tweetal aspecten getoetst. Het eerste aspect betreft het gebruik van het instrument. Hoe eenvoudig en eenduidig is het instrument in te vullen? Het tweede aspect is de bruikbaarheid van de resultaten van het instrument. Zijn deze resultaten herkenbaar, geven ze daadwerkelijk inzicht in de status van het continuïteitsbeheer?

1.6.5. Ethische aspecten

Business Continuity Management in ziekenhuizen kan een beladen onderwerp zijn. Er is daarom voor gekozen om de interviews anoniem te verwerken, uitsluitend voor het onderzoek te gebruiken en niet verder te publiceren. Uitkomsten van het onderzoek zullen wel openbaar gepubliceerd worden, maar hierbij zal herleidbaarheid naar individuele personen worden voorkomen.

1.7. De opdrachtgever

Het afstudeeronderzoek is verricht in opdracht van het UMC Utrecht. Met bijna 10.000 medewerkers is het UMC Utrecht één van de grootste zorginstellingen in Nederland.

Het Universitair Medisch Centrum Utrecht (UMC Utrecht) bestaat uit:

- Het Academisch Ziekenhuis Utrecht (AZU)
- Het Wilhelmina Kinderziekenhuis (WKZ)
- De Medische Faculteit van de Universiteit Utrecht

Kernactiviteiten van het UMC Utrecht zijn het verrichten van toonaangevend wetenschappelijk onderzoek, het bieden van 'state of the art' zorg en het verzorgen van opleiding aan studenten, (bio)medische onderzoekers, artsen en andere zorgverleners.[10]

2. Business Continuity Management

In dit hoofdstuk volgt een verdere verkenning van het concept Business Continuity Management. Om onderzoek te kunnen doen naar een beoordelingsinstrument voor BCM is het belangrijk inzicht te hebben in de diverse aspecten van continuïteitsbeheer. Hierbij zal ook regelgeving rondom BCM nadrukkelijk aan bod komen.

Er zijn een aantal factoren te noemen welke de toenemende belangstelling voor BCM verklaren. Zo hebben de aanslagen van 11 september 2001 in de VS, maar bijvoorbeeld ook de gevolgen van orkaan Katrina pijnlijker de kwetsbaarheid van bedrijfsprocessen bij rampen blootgelegd. Ook zijn bedrijfsprocessen steeds vaker kritisch afhankelijk geworden van complexer wordende informatiesystemen. Ketenintegratie, zoals bij supply chain management, maakt bedrijfsprocessen, ook over de grens van één organisatie, uitermate kwetsbaar voor uitval van systemen. De toenemende aandacht vertaalt zich in nationale en internationale regelgeving rondom informatiebeveiliging en continuïteitsbeheer.

2.1. **Begripsdefinitie**

Het begrip Business Continuity Management en de Nederlandse vertaling 'continuïteitsbeheer' is in dit rapport al een aantal keer gevallen. Een overzicht van een aantal definities van BCM:

Het Amerikaanse 'Disaster Recovery Journal' [11] kent een uitgebreide samenvatting van begrippen rondom continuïteitsbeheer. Business Continuity Management wordt als volgt beschreven:

"A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. The management of recovery or continuity in the event of a disaster. Also the management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date."

Bovenstaande omschrijving wordt ook gebruikt door de Business Continuity Planning Workgroup for Healthcare Organizations (BCPWHO) [12]. Een bijna gelijke definitie wordt ook gebruikt door 'the Business Continuity Institute' (theBCI.org) [13]

ITIL beschrijft het eigen IT Service Continuity Management als ondersteuning van het overkoepelende Business Continuity Management. BCM wordt hierbij beschreven als

"Business Continuity Management (BCM) is betrokken bij het analyseren en beheersen van risico's zodat de organisatie te allen tijde een minimaal noodzakelijke productiecapaciteit en/of dienstverlening kan waarborgen. Het BCM-proces tracht risico's tot een acceptabel niveau te beperken en maakt

plannen voor het herstel van de zakelijke activiteiten, mocht een onderbreking daarvan zich voordoen als gevolg van een calamiteit. “[14]

In Nederland houdt het adviesbureau “Verdonck, Klooster & Associates” (VKA) zich nadrukkelijk bezig met Business Continuity Management. Naomi Smit deed in opdracht van VKA onderzoek en gebruikt hierbij de definitie van BCM welke door VKA zelf gedefinieerd is.

“Business Continuity Management encompasses the management process that aims to prevent severe disruptions in the business and to protect critical processes against the consequences of disruptions or disasters” [15]

In de verschillende omschrijvingen van BCM zijn een aantal kenmerken die hierin steeds terug komen.

- BCM is een management proces
- BCM is holistisch
- Bij BCM gaat het om het analyseren en beheersen van risico's
- Bij BCM gaat het om de herstelkracht van een organisatie bij calamiteiten
- Bij BCM gaat het om kritische bedrijfsprocessen

In de verschillende definities komen deze aspecten in min of meerdere mate aan bod. De veel gebruikte definitie van ‘Disaster Recovery Journal’ [11], dekt het meest volledig deze aspecten en zal dan ook in dit onderzoek gebruikt worden:

“A holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. The management of recovery or continuity in the event of a disaster. Also the management of the overall program through training, rehearsals, and reviews, to ensure the plan stays current and up to date.”

In hoofdstuk 1 is te lezen dat dit onderzoek zich richt op een deelgebied van het Business Continuity Management. In paragraaf 2.2 wordt de afbakening, beschikbaarheid van informatievoorziening, verder uiteengezet.

2.1.1. Verwante begrippen

In het licht van BCM wordt ook regelmatig over ‘**Disaster Recovery**’ en ‘**Contingency Planning**’ gesproken. Het gaat hier om de technologische aspecten van BCM. Dit wordt exacter verwoord in de volgende definitie van BCPWHO [12]:”

"The technological aspect of business continuity planning. The advance planning and preparation that is necessary to minimize loss and ensure continuity of the critical business functions of an organization in the event of disaster. SIMILAR TERMS: Contingency Planning; Business Resumption Planning; Corporate Contingency Planning; Business Interruption Planning; Disaster Preparedness."

Ook **crisismanagement** is een deelgebied van het ruimere BCM. Disaster Recovery Journal [11] heeft het bij crisismanagement over:

"The overall coordination of an organization's response to a crisis, in an effective, timely manner, with the goal of avoiding or minimizing damage to the organization's profitability, reputation, and ability to operate."

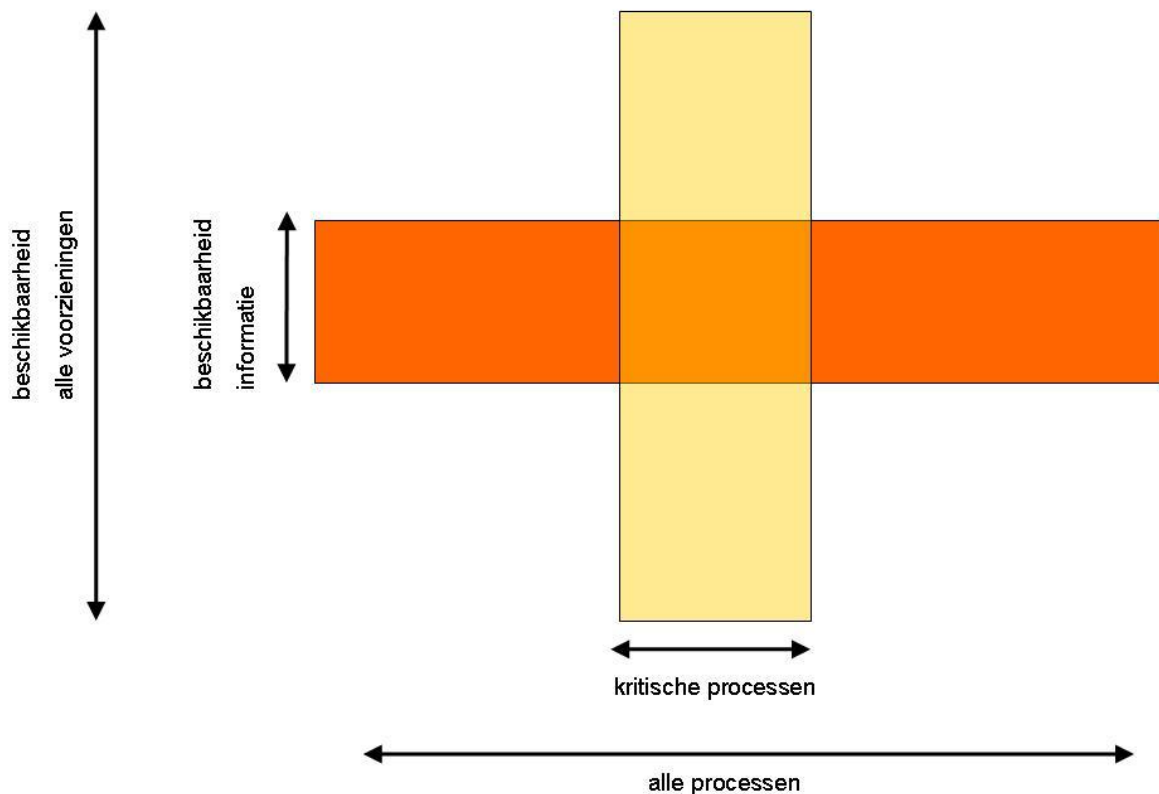
Misschien wel het meest tastbare resultaat van Business Continuity Management is het **Business Continuity Plan**. Business continuity planning is het *documenteren van de maatregelen en procedures* benodigd om als organisatie binnen een acceptabele tijd na een verstoring de meest kritische werkzaamheden weer te kunnen oppakken. [11]

Binnen het domein van Business Continuity Management zijn er een aantal veelgebruikte afkortingen. In NEN7510 [16] worden de termen '**Maximaal toegelaten uitvalsduur**' (**MUD**) en '**Maximaal toelaatbaar verlies aan gegevens**' (**MGV**) gebruikt. In Engelstalige literatuur wordt '**Maximum Tolerable Period of Disruption**' (**MTPD**) in plaats van MUD gebruikt. Het gaat hier om de maximale duur van uitval waarna de levensvatbaarheid van een organisatie (door financiële of reputatie consequenties) onomkeerbaar bedreigt wordt.

Vergelijkbare begrippen worden door de BCI.org [13] genoemd. De '**Recovery Point Objective**' (**RPO**) is de maximale duur tussen een incident en de laatste backup. Met andere woorden, bij een RPO van 6 uur, zal bij 'recovery' de laatste backup 6 uur of korter geleden moeten zijn gemaakt. De '**Recovery Time Objective**' (**RTO**) is de maximale benodigde tijd om te 'recovery' na een incident. Ofwel hoeveel tijd kan zonder de systemen gewerkt worden.

2.2. Informatiebeveiliging en continuïteitsbeheer

Informatiebeveiliging richt zich op de drie aspecten vertrouwelijkheid, integriteit en beschikbaarheid. [17] Waar het gaat om beschikbaarheid van informatie is er een overlap tussen informatiebeveiliging en Business Continuity Management. Waar informatiebeveiliging zich richt op beschikbaarheid van informatie, daar speelt bij BCM beschikbaarheid van veel meer voorzieningen dan uitsluitend informatie een rol. Denk hierbij bijvoorbeeld aan beschikbaarheid van bedrijfsruimte na een brand of beschikbaarheid van personeel bij een pandemie. Bovendien gaat het bij BCM primair om continuïteit van de kritische bedrijfsprocessen. Figuur 4 toont deze overlap. Zoals ook al in hoofdstuk 1 toegelicht is dit gedeelte van overlap onderwerp is van dit onderzoek.



Figuur 4 Beschikbaarheid informatie voor kritische processen

Verschillende, binnen de ICT gehanteerde frameworks, belichten het onderdeel van de 'IT-continuity'. Zo kent ITIL het 'IT Service Continuity Management' proces. Dit heeft tot doel ICT-diensten na een calamiteit zo snel mogelijk weer te herstellen. Om dit succesvol te kunnen doen is nodig dat Continuity Management afgestemd is op Business Continuity Management. [18]. Ook CobiT, het framework voor beheersing van it-processen en governance heeft specifieke aandacht voor Business Continuity. Verschillende processen binnen CobiT hebben betrekking op beschikbaarheid en continuïteit. Het voornaamste proces welke zich hiermee bezig houdt is het proces 'Ensure continuous service' binnen het aandachtsgebied 'Deliver and Support'. Daarnaast kent CobiT de zogenaamde Information Criteria. Het criterium 'availability' heeft hierbij een directe link naar continuity management. [19]

2.3. Inhoudelijke aspecten BCM

Vanuit de definitie kwam al naar voren dat BCM verschillende inhoudelijke aspecten kent. Voor het kunnen beoordelen van BCM is van belang deze verschillende aspecten te onderscheiden. Business Continuity Management wordt veelal beschreven als een cyclisch proces. Het volgt daarmee de Plan-Do-Check-Act cyclus welke, in het kader van kwaliteitsmanagement, actief werd gepromoot door W. Edwards Deming.[20] In figuur 5 is de 'Business Continuity Management lifecycle' afgebeeld, welke het proces in een bekende Britse norm op het gebied van BCM, BS25999, weergeeft. [21] In

paragraaf 2.4 zal dieper ingegaan worden op deze en andere normen en standaarden die betrekking hebben op BCM.



Figuur 5 Business Continuity Management Lifecycle [21]

In de volgende paragrafen worden achtereenvolgens de fasen analyse, maatregelen, evaluatie, testen en onderhoud nader toegelicht.

2.3.1. Analyse

De analysefase is een belangrijk onderdeel van het Business Continuity Management. Onderscheid kan hierbij gemaakt worden in:

- *risicoanalyse*, waarbij *bedreigingen* voor continuïteit worden vastgesteld worden en de *waarschijnlijkheid* dat deze bedreiging ook werkelijk tot een verstoring van de bedrijfsprocessen leidt. [16],[22],[23]
- *business impact analyse*, waarbij de impact van een verstoring wordt geïdentificeerd, gekwantificeerd en gekwalificeerd. [13] Het in kaart brengen van de eerder genoemde maximaal toegestane uitvalsduur (MUD) en het maximale toegestane verlies aan gegevens (MGV) maken ook deel uit van deze Business Impact Analyse.

2.3.2. Maatregelen

Er is een logische samenhang tussen de analyse-fase en de te nemen maatregelen. Pas als risico's vastgesteld zijn en bepaald is wat de impact van de bedreigingen is, kunnen bijbehorende maatregelen geformuleerd worden. Een verstorende gebeurtenis is in een aantal fasen op te delen.

Maatregelen kunnen worden uitgezet ten aanzien van deze verschillende fasen. Het type maatregel welke genomen dient te worden, hangt direct samen met de fase waarin de verstoring zich bevindt.

Helms heeft het over een Disaster Timeframe waarin de volgende fasen, en bijbehorende tijdvensters worden onderscheiden. [23]

- fase 1: T0-T1 Bedreiging, bedrijfsprocessen zijn nu nog onverstoord
- fase 2: T1-T2 Incident, storing wordt onderkend, bedrijfsprocessen komen tot stilstand
- fase 3: T2-T3 Schade, bedrijfsprocessen worden op een minimumniveau opgepakt
- fase 4: T3-T4 Herstel, in deze fase worden bedrijfsprocessen weer op het oude niveau gebracht

Een vergelijkbare indeling is de driedeling die Cazemier en Leegwater beschrijven. De eerste fase, die van 'Chaos; eerste hulp', vraagt crisisrespons, waarvoor een crisis management team benodigd is. De tweede fase, 'herstellen van cruciale processen', is de fase waarin een 'business continuity team' de activiteiten uitvoert. De laatste fase is die van 'recovery; back to normal', waarin processen weer worden teruggebracht tot normale operatie. [24]

2.3.3. Preventie en correctie

Afhankelijk van de fase van een incident zijn verschillende maatregelen denkbaar. Helms onderscheidt de volgende [23]

- Preventie, daarbij hoort ook het afwenden van een dreigend incident
- Detectie, het signaleren van een incident zodra dit zich voordoet
- Repressie, maatregelen om zo snel mogelijk te kunnen ingrijpen om schade te beperken
- Correctie, maatregelen om de problemen op te lossen en evt. schade te herstellen
- Evaluatie en correctie, maatregelen om de kennis rondom het incident te vergroten

Leegwater [6] noemt in zijn artikel een meer grofmazige indeling, te weten:

- preventieve maatregelen, zoals redundantie
- correctieve maatregelen, zoals noodprocedures en uitwijk
- geen maatregelen, met andere woorden het bewust accepteren van risico's

In de genoemde norm NEN7510, worden de volgende maatregelen onderscheiden.

“

- *Redundantie, het dubbel uitvoeren van voorzieningen*
- *Alternatieve werkwijze van het bedrijfsproces*
- *Uitstel van (onderdelen van) het bedrijfsproces*

- *Uitwijk van het bedrijfsproces en/of van voorzieningen*
- *Overige oplossingen*" [25]

In deze studie wordt gebruik gemaakt van de relatief grofmazige en eenvoudige indeling in preventieve en correctieve maatregelen.

Onder **preventieve** maatregelen wordt hierbij verstaan:

- maatregelen ter voorkoming van een incident, zoals redundantie, maar ook vroegtijdig signaleren van een dreigend incident

Onder **correctieve** maatregelen wordt verstaan:

- Maatregelen om de problemen op te lossen, alternatieve werkwijzen (noodprocedures) en maatregelen om weer de normale bedrijfsactiviteiten te hervatten.

2.3.4. Testen, onderhoud en evaluatie

De procesmatige benadering van Business Continuity Management kent ook een fase waarin analyse en maatregelen geëvalueerd worden. De BS25999 maakt hierbij onderscheid in testen, onderhoud en evaluatie. [26] De begrippen worden als volgt toegelicht:

Testen: Het op verschillende wijze oefenen van het continuïteitsplan. Denk hierbij aan technische testen, het op papier doorlopen van procedures tot een uiteindelijke integrale test in praktijk.

Onderhoud: het actueel houden van het continuïteitsplan in een dynamische omgeving.

Evaluatie: Het evalueren van business continuity moet er voor zorgen dat een organisatie ook een daadwerkelijk effectief BCM heeft. Onderscheiden worden hierbij de 'interne audit, een 'externe audit' en 'self-assessment', toetsing aan de hand van vragenlijsten.

2.4. Regelgeving, normen

Zoals al eerder naar voren kwam vertaalt de toenemende aandacht voor BCM zich ook in regelgeving en normen. Na 2001 is het aantal standaarden en voorschriften op het gebied van Business Continuity Management sterk toegenomen. Sommige zijn gericht op specifieke domeinen, zoals de financiële wereld (Sarbanes-Oxley, Basel), waarbij Business Continuity een onderdeel van de totale regelgeving vormt. Andere voorschriften kennen juist Business Continuity als hoofdonderwerp. Achtereenvolgens komen de belangrijkste algemene Business Continuity voorschriften en gezondheidszorgspecifieke regelgeving aan bod.

2.4.1. Algemene Business Continuity normen

In 2007 werd de lezers van het Britse Continuity Central gevraagd bekende 'business continuity standards' te noemen [27]. Van de 280 respondenten waren er 34% uit de VS, 31% UK en de overige uit andere delen van de wereld.

De bekendste standaarden:

- BS 25999-1:2006, Business continuity management, Part 1: Code of practice, Developed by: The British Standards Institution, Country: United Kingdom
- NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs, Developed by: The National Fire Protection Association, Country: United States
- HB 221:2004, Business Continuity Management, Developed by: Standards Australia, Country: Australia
- HB 292-2006, A practitioners guide to business continuity management, Developed by: Standards Australia, Country: Australia
- BS ISO/IEC 17799:2005, Code of practice for information security management, Developed by: The British Standards Institution, Country: United Kingdom

Niet in het lijstje uit het onderzoek, maar wel in diverse bronnen te vinden als belangrijke standaard op het gebied van Business Continuity:

- TR 19 : Technical Reference for Business Continuity Management (SPRING, Singapore)

Uit het onderzoek van Continuity Central kwam BS25999 hierbij overtuigend als meest bekende standaard naar voren. BS25999 wordt nog wel eens in een mond genoemd met PAS56. Deze **Public Available Standard** werd in 2003 door de British Standard Institution uitgegeven, vormt de voorloper van BS25999 en is hierdoor in 2006 vervangen.

In Nederland is de '*Code voor Informatiebeveiliging*' bekend. Dit is een vertaling door de NEN van een British Standard 7799, en uiteindelijk opgegaan in de eerder genoemde ISO 17799.

2.4.2. Normen BCM gezondheidszorg

Een vroege vorm van regelgeving met aandacht voor Business Continuity Management is HIPAA, de 'Health Insurance Portability and Accountability Act'. Deze is in 1996 door de Amerikaanse overheid ontworpen en in 2001 ook wettelijk vastgelegd. In de HIPAA zijn richtlijnen opgenomen die zorginstellingen verplicht om te voldoen aan data security en business continuity standaarden.[6] De impact van HIPAA voor de Amerikaanse gezondheidszorg is groot. De inschatting is dat de kosten hiervoor die van de 'Y2K preparedness' overstijgen. In combinatie met aanvullende maatregelen op het gebied van bescherming tegen aardbevingen, kunnen kleinere ziekenhuizen deze kosten niet meer opbrengen. [28]

Voor de Nederlandse gezondheidszorg is de norm NEN7510 ontwikkeld. Samen met het 'toetsbare voorschrift' NEN7511 zijn dit dé richtinggevende normen op het gebied van informatiebeveiliging in de zorgsector.

2.4.2.1. NEN7510 – NEN7511

NEN7510 houdt zich bezig met informatiebeveiliging in de zorg. Op de website van NEN7510 wordt informatiebeveiliging als volgt uitgelegd. *“Onder informatiebeveiliging in de zorg wordt verstaan: het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie die benodigd is om patiënten verantwoorde zorg te kunnen bieden. Naast het borgen van deze kwaliteitscriteria vereist deze norm ook dat de informatiebeveiligingsmaatregelen op controleerbare wijze zijn ingericht voordat kan worden gesproken over adequate informatiebeveiliging. De norm kan beschouwd worden als een kader.”* [29]

In NEN 7511-1, het toetsbaar voorschrift bij NEN 7510 voor complexe organisaties, is een hoofdstuk gewijd aan continuïteitsbeheer. In een aantal pagina's wordt op beknopte wijze het continuïteitsbeheer uiteengezet. [16] De volgende aspecten worden hierbij benoemd met betrekking tot continuïteitsbeheer

“Het continuïteitsbeheer moet maatregelen bevatten voor het:

- a) vaststellen en verminderen van risico's;
- b) beperken van de gevolgen van incidenten die schade toebrengen;
- c) tijdig hervatten van essentiële werkzaamheden.”

In een continuïteitsstrategie moet voor ieder bedrijfsproces een maximaal toegelaten uitvalduur (MUD) en een maximaal toelaatbaar verlies aan gegevens (MGV) worden vastgelegd.

Er dienen continuïteitsplannen te worden ontwikkeld en continuïteitsvoorzieningen geïmplementeerd. In de continuïteitsplannen moet duidelijk worden vastgelegd onder welke voorwaarden welke activiteiten uitgevoerd dienen te worden en welke personen op welk moment verantwoordelijk zijn. Een dergelijk plan dient tevens een eindverantwoordelijke te hebben.

Continuïteitsplannen dienen regelmatig getoetst te worden en onderhouden te worden. Bijwerken hiervan dient onderdeel te zijn van het wijzigingsproces in de organisatie.

Voor Nederlandse zorgorganisaties is NEN7510 in toenemende mate een belangrijke norm. Om aan te kunnen sluiten op het landelijk Elektronisch Patiënten Dossier moeten ziekenhuizen in de nabije toekomst voldoen aan de NEN 7510. Het landelijk EPD maakt het mogelijk om gegevens tussen verschillende zorgaanbieders uit te wisselen. Dit moet bijdragen aan een efficiëntere en veilige patiëntenzorg.

Waar de norm zelf vrij beknopt in gaat op continuïteitsbeheer, daar is het handboek NEN 7510 veel uitgebreider. Dit handboek vormt een uitgebreide toelichting en bevat diverse voorbeelden welke bruikbaar zijn bij implementatie. Later in dit verslag wordt ingegaan op checklists die in dit handboek worden gebruikt.[25] Interpay, de Nederlandse bancaire organisatie, tegenwoordig opgegaan in Equens, deed in 2006, in opdracht van VWS onderzoek naar informatiebeveiliging in de zorg. Rondom continuïteitsbeheer adviseerde Interpay om de richtlijnen uit NEN7510 landelijk te formaliseren en centraliseren. Als voorbeeld noemt Interpay hierbij het jaarlijks testen van uitwijkscenario's. [30]

2.5. BCM en gezondheidszorg

Het proces van Business Continuity Management in de gezondheidszorg verschilt niet wezenlijk van BCM in andere sectoren. Wel is een aantal factoren waardoor het vraagstuk rondom Business Continuity juist in de zorg erg belangrijk is geworden.

Een toenemende afhankelijkheid van complexere informatie en communicatiesystemen en de hierin opgeslagen data. In een uitgebreid onderzoek in 2006 onder vijf Amerikaanse ziekenhuizen zijn de belangrijkste 'neveneffecten' bij het gebruik van 'Computerized Provider Order Entry' in kaart gebracht.[31] Het gaat hierbij om systemen zoals ordermanagement en elektronisch medicatie voorschrijfsystemen, welke ook in Nederland belangrijke elementen in het EPD vormen. Eén van de gevonden neveneffecten was de 'overafhankelijkheid van technologie'. Geconstateerd wordt dat basale medische zorg niet meer verleend kan worden zonder technologie, en dat continuïteitsmaatregelen dan ook noodzaak zijn. In een vervolgonderzoek wordt het belang en de omvang van deze 'neveneffecten' verder uitgediept. [32] Hieruit blijkt dat 83% van de ondervraagde medewerkers uit de ziekenhuizen de afhankelijkheid van technologie een belangrijke 'nevenconsequentie' vindt. Daarnaast worden een aantal andere bevindingen gedaan. Zo zijn er vaak wel noodvoorzieningen op papier, maar hebben veel medewerkers hier nooit mee gewerkt. Ook blijkt bij het weer 'online' komen van systemen er veel inspanning nodig is om de papieren verslaglegging weer digitaal te krijgen. Een belangrijke conclusie is dan ook dat uitval van zorgsystemen leidt tot een 'beheerde chaos met een grote negatieve impact op productiviteit'. [32]

Wet en regelgeving. De eerder besproken HIPAA en NEN7510 zijn voorbeelden van wet- en regelgeving welke een specifieke invulling voor de gezondheidszorg kennen.

Wellicht het belangrijkste verschil met andere sectoren is dat in de gezondheidszorg mensenlevens direct afhankelijk zijn van de continuïteit van bedrijfsvoering. Of zoals Mark Roman het in zijn artikel over "business continuity in healthcare" verwoord:

"Although each industry has a unique set of challenges when responding to business disruptions, continuity of operations in healthcare goes far beyond maintaining or recovering basic business operations and IT systems—it is a matter of life and death." [33]

Waar het om 'vitale' bedrijfsprocessen in de gezondheidszorg gaat kan dit dan in een aantal gevallen niet letterlijk genoeg worden opgevat. In de norm NEN7510 worden rondom een aantal categorieën de kritische bedrijfsprocessen genoemd. Het gaat hierbij om patiëntenzorg, onderzoek, onderwijs en ondersteunende processen. Binnen de scope van mijn onderzoek richt ik mij primair op het deelgebied van de patiëntenzorg. Hierin worden door de NEN in het handboek NEN7510 de volgende processen genoemd [34]:

- Uitvoeren van operaties
- Verlenen van Intensive Care aan patiënten
- Beademen van patiënten
- Bewaken en monitoren van patiënten
- Zorg verlenen aan patiënten in isolatie
- Verlenen van spoedeisende hulp (SEH)
- Leveren en beheren van medicatie (Apotheek)
- Inschrijven van patiënten
- Doen van bepalingen in laboratoria ten behoeve van patiëntenzorg
- Uitvoeren van diagnostische handelingen (röntgen)
- Leveren en beheren van bloed en bloedproducten (bloedbank).

Van deze processen zal de maximale uitvalsduur minuten tot enkele uren mogen bedragen. In vele gevallen is gegevensverlies in het geheel niet toelaatbaar. Opgemerkt wordt dat deze processen in de patiëntenzorg veelal afhankelijk zijn van ondersteunende processen. Een opsomming van ondersteunende processen volgens NEN7510 [34] :

- Steriliseren van instrumenten en andere middelen, [Centrale Sterilisatie Afdeling (CSA)]
- Verzorgen van voeding voor patiënten, bezoekers en medewerkers (Keuken)
- Leveren en beheren van medische gassen (zuurstof, stoom)
- Beheren en transporteren van bedden [Beddencentrale]
- Leveren en beheren van nutsvoorzieningen (gas, water, stroomvoorziening, luchtbehandeling, koeling, stadsverwarming)
- Leveren en beheren van ICT (netwerk en centrale computers), informatievoorziening
- Leveren en beheren van communicatievoorzieningen
- Leveren en beheren van vitale kantoorvoorzieningen (o.a. tekstverwerking en email)
- Beheren en bewaken van "onderdruk" en "overdruk" ruimten
- Leveren van managementinformatie
- Leveren en beheren van logistieke voorzieningen
- Leveren en beheren van telecommunicatie en telefonie
- Administreren van salarissen
- Beveiligen en beheren van ruimten (o.a. zaalreservering).

Duidelijk mag zijn dat niet al deze ondersteunende processen direct kritisch zijn voor het leveren van patiëntenzorg.

2.6. Stakeholders

Gezien het holistische karakter van Business Continuity Management is het niet verwonderlijk dat er ook verschillende betrokkenen en belanghebbenden bij dit proces zijn.

Het eerder genoemde framework COBIT werkt met een zogenaamd RACI diagram om stakeholders in kaart te brengen. Hierin wordt uitgezet welke functionarissen voor activiteiten **Responsible**, **Accountable**, **Consulted** en/of **Informed** zijn. Voor de activiteiten rondom continuïteitsbeheer worden de volgende functies genoemd.

- CEO
- CFO
- Business Executive
- CIO
- Business Process Owner
- Head Operations
- Chief Architect
- Head Development
- Head IT Administration
- PMO (Project Management Office)
- Compliance, Audit, Risk and Security

De Business Executive en Business Process Owner laten zich in de praktijk van de gezondheidszorg vertalen in vertegenwoordigers van Medische staf en Zorgverlening. Al eerder kwam naar voren dat het bij continuïteitsbeheer in de gezondheidszorg een zaak van 'leven of dood' kan zijn. Daarmee heeft continuïteitsbeheer dan ook een belangrijke relatie met het domein van de patiëntveiligheid.

2.7. Samenvatting

In Business Continuity Management staat continuïteit van bedrijfsprocessen centraal. Er is een overlap tussen Business Continuity Management en Informatiebeveiliging. Juist dit gebied, continuïteitsbeheer van informatievoorziening is ook onderwerp van dit onderzoek. Business Continuity Management is een cyclisch proces waarin fasen van 'analyse', 'maatregelen' en 'onderhoud, test en evaluatie' worden onderscheiden. Een toenemende belangstelling voor BCM is ook zichtbaar in ontwikkeling van regelgeving en normen. Vanuit internationaal perspectief is de British Standard voor Business Continuity, BS25999, het meest genoemd. Op het gebied van informatiebeveiliging voor de Nederlandse gezondheidszorg is NEN7510 richtinggevend. Business

Continuity in de gezondheidszorg is niet wezenlijk verschillend van andere bedrijfstakken. Wel speelt binnen de gezondheidszorg nadrukkelijk het thema patiëntveiligheid. Gezien het holistische karakter van Business Continuity Management, zijn er veel belanghebbenden te noemen in dit proces. Zowel vanuit de business als de ICT-organisatie, in de verschillende niveaus van strategisch tot operationeel.

3. Beoordelingsinstrument voor BCM

Om te kunnen bepalen of de juiste maatregelen voor continuïteitsbeheer zijn genomen is een beoordelingsinstrument nodig. In dit hoofdstuk zal ingegaan worden op de definitie van een 'beoordelingsinstrument'. Ook zal ingegaan worden op maturity modellen. Vervolgens een aantal voorbeelden van bestaande beoordelingsinstrumenten voor het meten van Business Continuity Management.

3.1. *Een beoordelingsinstrument*

In de onderzoeksvraag is aangegeven wat gemeten dient te worden in het kader van BCM. Het gaat om:

- welke maatregelen zijn genomen voor het vaststellen en verminderen van risico's
- beperken van gevolgen van incidenten
- tijdig hervatten van werkzaamheden

Echter het meten is geen doel op zich. Dit komt ook duidelijk naar voren uit de interviews gehouden met stakeholders in het UMC Utrecht. Aan het normerend aspect van het meetinstrument wordt veel waarde gehecht. Juist dit normerende aspect kan ervoor zorgen dat duidelijk wordt welke aspecten in het continuïteitsbeheer onderbelicht zijn. Bovendien kan na verbeteracties worden bepaald of de norm nu wel gehaald wordt. Dat is de reden dat er in dit onderzoek gekozen is voor de term 'beoordelingsinstrument'.

Overigens worden voor soortgelijke instrumenten verschillende termen zoals 'meetinstrument', 'beoordelingsinstrument', 'audit tool' en '(self)assessment-tool' gebruikt.

De resultaten van een beoordeling kunnen worden weergegeven in een model. Een model is hierbij gedefinieerd als een 'representatie van een deel van de wereld'. [35] Een veelgebruikt model is het 'maturity model'. Alom bekend is het Capability Maturity Model for Software (CMM), later vervangen door CMM Integration. [36] De eerste versies van dit model zijn door het 'software engineering institute' gemaakt in 1987. Inspiratie werd hierbij opgedaan uit het succes van Total Quality Management en eerdere maturity Frameworks van Philip Crosby en IBM. [37]

Naomi Smit deed onderzoek naar een maturity model voor Business Continuity. Gebaseerd op omschrijvingen van Paulk, programma manager van CMM en Mingay onderzoeker bij Gartner, komt zij tot de volgende definitie voor maturity model. [15]

“A maturity model is a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached.”

Bovenstaande definitie, maakt duidelijk dat het bij een maturity model gaat om het bereiken van een bepaald niveau en het werken naar een gewenst hoger niveau. Het model kan hierbij ook gebruikt worden om verschillende organisaties met elkaar te vergelijken.

Het afbeelden van een volwassenheidsniveau van de *totale organisatie* is niet het doel van dit onderzoek. Het gaat hier om het beoordelen van continuïteitsbeheer rondom informatievoorziening van een *bedrijfsproces*. Niettemin vormen de maturity modellen en bijbehorende meetinstrumenten een bruikbaar voorbeeld voor een beoordelingsinstrument continuïteitsbeheer.

Een beoordelingsinstrument is niet hetzelfde als een *Business Continuity Plan* (BCP). Bij een BCP gaat het om het ontwikkelen en documenteren van de activiteiten rondom continuïteitsbeheer. Bij een beoordelingsinstrument gaat het om de vaststelling of het continuïteitsbeheer goed is ingericht. Met betrekking tot continuïteit rondom zorgkritische ICT is het continuïteitsplan van het Erasmus MC een goed voorbeeld. [38]

3.2. *Bestaande beoordelingsinstrumenten*

In dit onderzoek is de keuze gemaakt om bestaande beoordelingsinstrumenten te toetsen op hun bruikbaarheid. De zoektocht naar deze instrumenten heeft zich gericht op vrij toegankelijke instrumenten, veelal via Internet in te zien. Een andere categorie zijn de meetinstrumenten die weliswaar niet openbaar gepubliceerd zijn, maar wel toegankelijk zijn via contacten binnen de ziekenhuizen. Niet meegenomen zijn beoordelingsinstrumenten die alleen inzichtelijk waren na aankoop van deze lijsten. Sommige gevonden beoordelingsinstrumenten, zoals die van zakenbank Meryll Lynch [39] hadden een dusdanig andere scoping – niet de eigen processen, maar die van leveranciers – dat zij buiten de analyse zijn gehouden.

Enkele van de gevonden meetinstrumenten zijn primair gericht op continuïteitsbeheer, anderen kennen een bredere focus (bijvoorbeeld informatiebeveiliging). Van deze instrumenten is uitsluitend het deel rondom continuïteitsbeheer belicht. Beoordelingsinstrumenten behorende bij de eerder besproken maturity modellen, zijn ook meegenomen in deze analyse. Onderzocht zijn:

- Monitor Informatiebeveiliging 2.008
- NEN7510 checklist continuïteitsplanning
- Business Continuity Maturity Model
- BCI PAS56 Audit Workbook v2.0
- Code voor informatiebeveiliging

3.2.1. Monitor informatiebeveiliging 2.008

De monitor 'Informatiebeveiliging in de zorg' is een uitgebreide online vragenlijst welke is opgesteld naar NEN 7510. De Monitor informatiebeveiliging is ontwikkeld door de acht Universitair Medisch Centra en gepubliceerd door KPMG Qubus Competence Center.[40] Met behulp van deze monitor kunnen de Universitair Medisch Centra zelf NEN 7510-audits houden en de resultaten onderling vergelijken.

Hoofdstuk 9 van deze vragenlijst is volledig aan 'continuïteitsbeheer' gewijd. Het gaat om een 28-tal vragen in de volgende categorieën:

9.1 Aspecten van continuïteitsbeheer

9.1.1 Het proces van continuïteitsbeheer

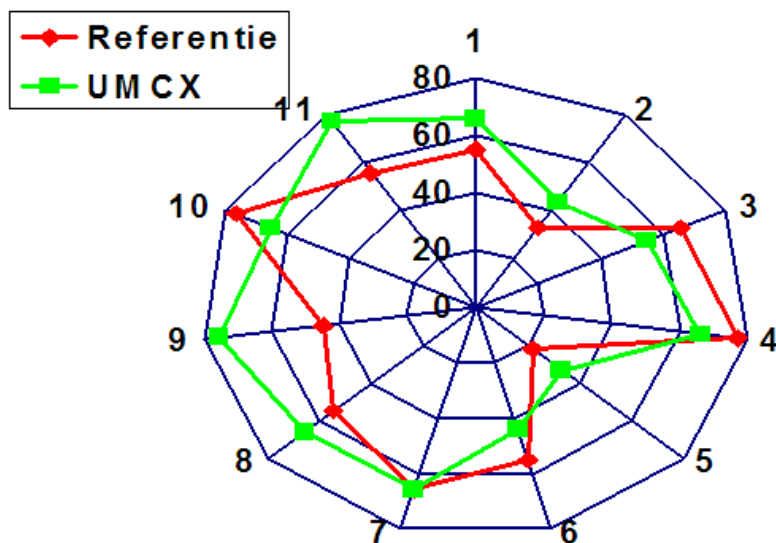
9.1.2 Bepalen van de continuïteitsstrategie

9.1.3 Ontwikkelen en implementeren van continuïteitsvoorzieningen en –plannen

9.1.4 Structuur voor continuïteitsplannen

9.1.5. Toetsen, bijwerken en evalueren van continuïteitsplannen

Antwoordmogelijkheden zijn 'Ja', 'Nee', 'Gedeeltelijk', zonder ruimte voor toelichting. De vragenlijsten kennen ook een vertaling naar een waardering van de getoetste aspecten, echter deze is niet vrij beschikbaar. Het resultaat toont zich als een 'radardiagram', zoals afgebeeld in figuur 6. Per hoofdstuk van NEN7510 wordt hier een score tussen 0 en 100% toegekend. Voor de ziekenhuizen die deelnemen aan het onderzoek is zowel de eigen score, als de gemiddelde score van de overige ziekenhuizen zichtbaar. De afgebeelde score in figuur 6 is slechts als voorbeeld en representeert geen werkelijke score.



Figuur 6 Diagram Monitor Informatiebeveiliging

3.2.2. NEN7510 checklist continuïteitsplanning

Het handboek NEN7510 geeft een toelichting op NEN 7510 en 7511 en bevat verschillende handleidingen en voorbeelden om direct toe te passen. [25] Onderdeel van deze handleiding is de checklist continuïteitsplanning. Deze is bedoeld als leidraad bij inrichting van continuïteitsplanning voor een bedrijfsproces of ICT-omgeving. Er kan met 'Ja', 'Nee', 'Gedeeltelijk' en 'Onbekend' beantwoord worden en bij ieder antwoord is ruimte voor opmerkingen.

In de checklist staan 30 vragen rondom de volgende onderwerpen onderverdeeld in de volgende aandachtsgebieden:

- Taken en verantwoordelijkheden
- Vaststellen van een calamiteit
- Middelen en faciliteiten
- Procedures en documentatie
- Testen van het calamiteitenplan
- Overleg, communicatie en rapportage

3.2.3. Checklist Code voor informatiebeveiliging

Nen7510 is gebaseerd op de 'code voor informatiebeveiliging'. De code voor informatiebeveiliging is internationaal bekend onder ISO/IEC 17799. Ernst Oud publiceerde een uitgebreide checklist beveiligingsbeleid, gebaseerd op deze code voor informatiebeveiliging. [41] Deze checklist is op

internet te downloaden via Kennisnet, de ICT-ondersteuningsorganisatie voor het onderwijs. [42]
Hoofdstuk 11 van de checklist behandelt het continuïteitsmanagement.

11.1.1 Het proces van continuïteitsmanagement (17 vragen)

11.1.2 Bedrijfscontinuïteit en analyse van mogelijke gevolgen (6 vragen)

11.1.3 Het schrijven en invoeren van continuïteitsplannen (3 vragen)

11.1.4 Structuur van de continuïteitsplanning (10 vragen)

11.1.5 Testen, onderhouden en evalueren van continuïteitsplannen (24 vragen)

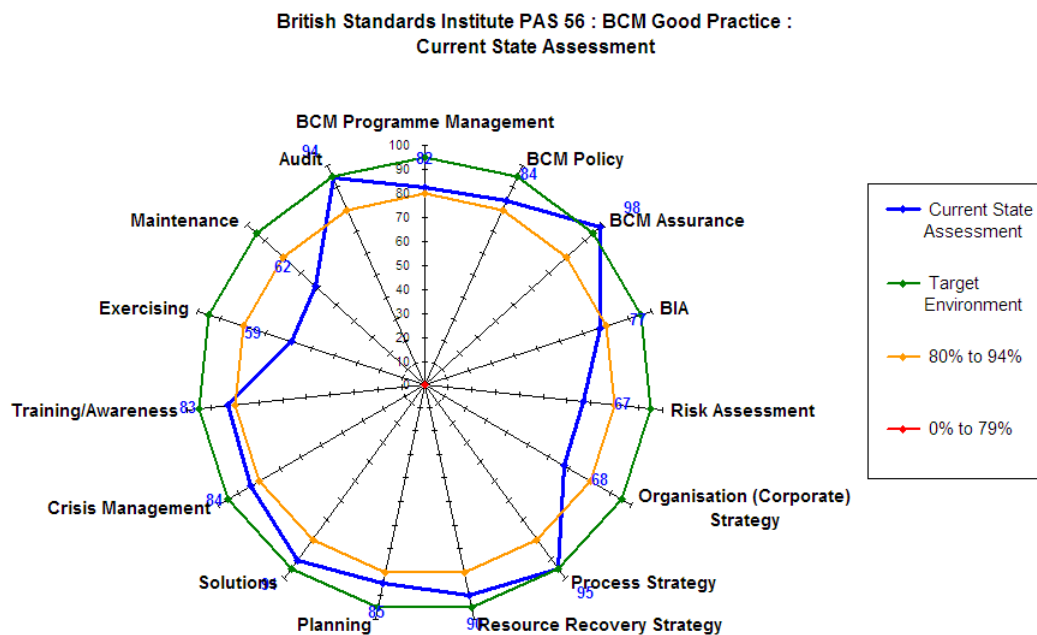
Op de vragen kan een antwoord gegeven in vier categorieën (Ja, Nee, Gedeeltelijk, Onbekend), zonder verdere ruimte voor toelichting.

3.2.4. BCI PAS56 Audit Workbook v2.0

Bij introductie van PAS56 publiceerde de British Continuity Institute (BCI) op de website een audit tool.[43] Dit instrument, geïmplementeerd in een Excel spreadsheet, maakt het mogelijk een 'gap analyse' te doen op het continuïteitsbeheer. Hoewel BCI deze tool, om auteursrechtelijke redenen, weer van de website verwijderd heeft, is deze op internet op verschillende plaatsen nog wel te vinden.[44] [45] De audit tool volgt de evaluatiecriteria zoals deze in de 'Publicly Available Specification' staan beschreven. In de excelsheet moet van ieder aspect in een percentage (0, 20, 40, 60, 80, 90, 100%) worden aangegeven in hoeverre hieraan wordt voldaan. Naast de score, zijn aparte antwoordvelden opgenomen voor opmerkingen, suggesties voor verder onderzoek, verbeterplannen met eigenaar en einddatum. Voor iedere stap in de levenscyclus (totaal 6 stappen) van BCM, dienen vragen, in totaal 186, te worden beantwoord. Uiteindelijk worden deze doorgerekend en gewogen, zodat van ieder hoofdaspect kan worden bepaald of hieraan wordt voldaan. De percentages vertalen zich in drie categorieën, groen, geel en rood.

95% - 100% Compliance
80% - 94% Compliance
0% - 79% Compliance

Zoals in figuur 7 te zien is, levert een ingevuld audit tool een grafische weergave van de staat van de verschillende te scoren aspecten.



Figuur 7 PAS 56 - Current State Assessment [43]

Bij Delta Lloyd is deze tool ook in gebruik. Omdat de percentages lastig eenduidig zijn te interpreteren, is bij Delta Lloyd besloten om een beschrijving van de verschillende percentages te geven.[46] Hierbij valt op dat de omschrijvingen, zoals gekozen door Delta Lloyd, exact overeenkomen met de omschrijving van de maturity levels gebruikt in het Business Continuity Maturity Model. Dit model wordt in de volgende paragraaf beschreven.

3.2.5. Business Continuity Maturity Model

Virtual Corp is een Amerikaans bedrijf voor software en consultancy op het gebied van Business Continuity. Deze organisatie heeft een toonaangevend maturity model met betrekking tot Business Continuity ontwikkeld, het Business Continuity Maturity Model (BCMM). Het model is als een 'open access version' in Spaans- of Engelstalig te downloaden van de website van Virtual Corp. In een document van 71 pagina's worden de verschillende levels toegelicht en beschreven hoe een 'self-assessment' kan worden gedaan. Net als bij de PAS56 audit workbook gaat het om het scoren van percentages bij de verschillende aspecten. [47] In figuur 8 staan zowel de 6 maturity levels als de 8 'corporate competences' benoemd, welke in het maturity model de assen van de matrix vormen. Ieder maturity level kent een omschrijving, zoals 'Self-Governed' voor Level 1. Daarnaast is er een alternatieve omschrijving per level, de zogenaamde 'Athlete Analogy'. Ten slotte is er ook een driedeling gemaakt, die de volwassenheid van de organisatie in meer vergelijkende termen uitdrukt. Level 1 en 2 staan voor 'Organization at Risk', Level 3 en 4 voor 'Competent Performer', en voor de twee hoogste levels is het label 'Best of Breed' gereserveerd. Virtual Corp stelt dat deze alternatieve omschrijvingen voor meer duidelijkheid zorgen. [47] Het uiteindelijke niveau voor iedere cel in de matrix wordt uitgedrukt in 'very low', 'low', 'medium', 'high'

The BCMM [®]		Increasing Business Continuity Competency Maturity				
Standard Reference Chart						
Maturity Model Levels	Level 1 Self-Governed	Level 2 Supported Self-Governed	Level 3 Centrally Governed	Level 4 Enterprise Awakening	Level 5 Planned Growth	Level 6 Synergistic
Athlete Analogy	Able to Crawl	Able to Walk	Able to Run	"Fit" Runner	Competitive Runner	Olympic Runner
Comparative Model	Organization "At Risk"		"Competent" Performer		"Best of Breed"	
Corporate Competencies		General Attributes of an Organization at Each Maturity Level				
Leadership	VL	L	M	H	H	H
Employee Awareness	VL	L	L	M	H	H
BC Program Structure	VL	L	L	M	H	H
Program Pervasiveness	VL	L	L	L	M	H
Metrics	VL	L	M	M	H	H
Resource Commitment	VL	L	M	H	H	H
External Coordination	VL	L	L	M	H	H
BC Program Content	VL	L	M	H	H	H

Figuur 8 BCMM standard reference chart [47]

Op de website van Virtual Corp is een survey beschikbaar, welke inzicht geeft in het volwassenheidsniveau van de organisatie met betrekking tot Business Continuity Management.[48] De survey, welke bestaat uit 21 vragen, is onderverdeeld in de volgende hoofdstukken:

- User Characteristics (6 vragen)
- Your Current State-of-Preparedness (5 vragen)
- Enterprise Implementation Prerequisites (6 vragen)
- BCM Implementation Reality (4 vragen)

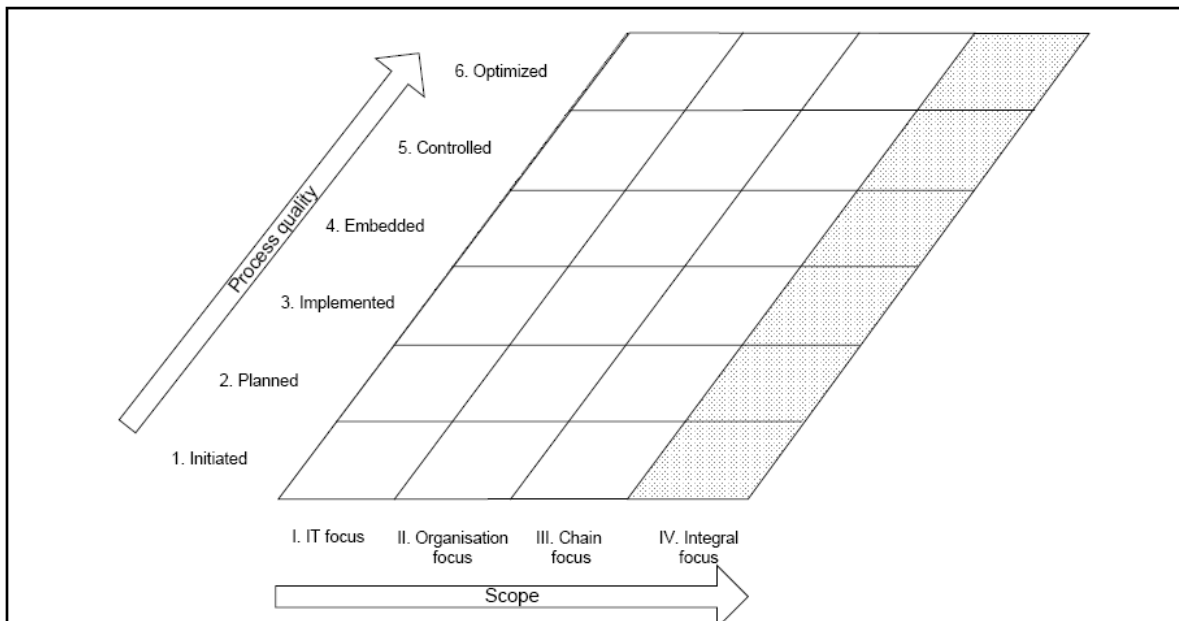
Het gaat hierbij steeds om meerkeuze vragen, waarbij geen mogelijkheid is om een toelichting bij de antwoorden te registreren.

Na het invullen van de vragenlijst wordt een maturity niveau gepresenteerd. In de documentatie van BCMM staat uitgelegd hoe de berekening tot stand is gekomen.

3.2.6. Een Nederlands Business Continuity Maturity Model

Naomi Smit heeft in haar onderzoek naar een Maturity Model voor Business Continuity Management een aantal maturitymodellen gecombineerd. [15] In het onderzoek worden twee bestaande maturity modellen getoetst, maar deze voldoen niet aan de door Smit gestelde eisen. Het gaat hierbij om het zojuist besproken BCMM en het 'Gartner BCP Maturity Model, welke is gebaseerd op het maturity model van CobiT. De beide modellen geven, volgens dit onderzoek, te weinig 'action-based' adviezen en zijn niet gebaseerd op erkende 'best-practice' methodologiën.

Het door Smit ontwikkelde maturity model, afgebeeld in figuur 9, kent zes maturity levels, welke voor 4 deelgebieden ('scope') kunnen worden benoemd.



Figuur 9 Maturity Model for BCM - Naomi Smit [15]

De bijbehorende quick-scan is echter niet openbaar beschikbaar, waardoor dit instrument niet in aanmerking kwam om als referentie-instrument te worden opgenomen. [15]

3.3. Concept criteria beoordelingsinstrument

Om te kunnen beoordelen welk bestaand beoordelingsinstrument het meest geschikt is om toe te passen in de UMC Utrecht situatie, zijn toetsingscriteria nodig. Het bepalen van de criteria is in eerste instantie vanuit de literatuur en de scoping van de onderzoeksvraag gedaan. Deze conceptcriteria zullen in deze paragraaf nader toegelicht worden.

De gevonden criteria zijn vervolgens voorgelegd aan de diverse stakeholders binnen het UMC Utrecht. Dit heeft geleid tot een verdere aanpassing en uitbreiding van de criteria. Over de methode van voorleggen en het resultaat gaat hoofdstuk 4.

De criteria zijn in drie categorieën onderverdeeld.

Inhoudelijke aspecten

Het beoordelingsinstrument dient zich op alle inhoudelijke aspecten te richten die met continuïteitsbeheer te maken hebben. Het gaat hierbij om de verschillende fasen in het continuïteitsproces, de analysefase, maatregelen, evaluatie en organisatie.

Kwaliteitscriteria

Deze criteria hebben betrekking op kwaliteiten en eigenschappen van het beoordelingsinstrument. . In zijn boek over kennisverwerving in de empirische wetenschappen beschrijft onderzoeker Foeke van

der Zee een aantal eigenschappen van meetinstrumenten. [49] Meet het instrument bijvoorbeeld wat het moet weten (validiteit) en is het instrument discriminerend naar goede en slechte bevindingen (normerend)? Het gaat hier dus om criteria die niet specifiek voor een beoordelingsinstrument voor BCM zijn, maar meer voor meet- en beoordelingsinstrumenten in z'n algemeenheid.

Scopingscriteria

De toepassing van het beoordelingsinstrument, zoals in de doelstelling van het onderzoek is geschetst, stelt bepaalde eisen aan het instrument. Deze eisen hebben te maken met de scoping van het instrument. Zo moet het instrument beoordelen op continuïteitsbeheer van *informatievoorziening* en bijvoorbeeld niet continuïteit van bijv. watervoorziening. In hoofdstuk 1 wordt als mogelijke toepassing van het instrument genoemd om een meting te doen tijdens een implementatietraject van informatiesystemen. Die toepassing impliceert dat het meetinstrument al na één meting een zinvol resultaat moet kunnen tonen. Dit in tegenstelling tot resultaten die vooral nuttig zijn wanneer het verloop na meerdere metingen duidelijk wordt.

In onderstaande tabel 1 staan de criteria opgesomd, voorzien van nadere toelichting en verwijzing naar de bron waar deze beschreven staat.

Tabel 1 Concept criteria beoordelingsinstrument

Inhoudelijke aspecten		
<i>Risicoanalyse</i>		
<i>Vaststellen bedreigingen</i>	Het benoemen van mogelijke bedreigende incidenten voor continuïteit van het betreffende bedrijfsproces	[22], [16]
<i>Vaststellen waarschijnlijkheid</i>	Het benoemen van de waarschijnlijkheid dat het bedreigende incident plaatsvindt	[23]
<i>Business Impact Analyse</i>		
<i>Vaststellen impact</i>	Identificeren, kwantificeren en kwalificeren van schade ontstaan door verstoring van bedrijfsproces	[13], [22]
<i>Vaststellen MUD</i>	Vaststellen maximale duur van verstoring proces	[16]
<i>Vaststellen MGv</i>	Vaststellen maximaal toelaatbaar verlies aan gegevens	[16]
<i>Maatregelen</i>		
<i>Vaststellen preventieve maatregelen</i>	Maatregelen ter voorkoming van verstoring of afwending dreiging van incident	[6]
<i>Vaststellen correctieve maatregelen</i>	Maatregelen om in het geval van een incident zo snel mogelijk bedrijfsproces te kunnen hervatten en evt. schade te herstellen	[6]

Evaluatie		
<i>Testen maatregelen</i>	Het periodiek testen van maatregelen	[22]
<i>Onderhoud maatregelen</i>	Bijstellen van maatregelen ingebed in reguliere wijzigingsbeheerprocessen	[22]
Criterium	Omschrijving	Bron
Kwaliteitsaspecten		
<i>Efficiëntie</i>	De juiste vragen worden gesteld, zodat meting efficiënt plaatsvindt.	[49]
<i>Objectief</i>	Onderzoeker mag geen invloed hebben op het resultaat. Meting uitgevoerd door verschillende personen moet zelfde uitslag geven.	[49]
<i>Normerend</i>	het meetinstrument moet voldoende discriminerend vermogen hebben. Het moet een meetlat zijn waardoor vergelijking tussen verschillende metingen mogelijk worden	[49]
<i>Valide</i>	De resultaten van de test zeggen daadwerkelijk iets over het gemeten onderwerp (ic continuïteitsbeheer)	[49]
<i>Voldoen aan regelgeving</i>	Wordt in het meetinstrument getoetst op de aspecten zoals die in de NEN-norm voor informatiebeveiliging (NEN7510) voor continuïteitsbeheer zijn vastgesteld? Deze norm is straks leidend bij het landelijk EPD.	[29]
Scope van meetinstrument		
<i>Metten op niveau bedrijfsproces (detailniveau)</i>	De scope van de meting is het bedrijfsproces (een BCM meting kan bijv. ook op het niveau van de organisatie als geheel plaatsvinden)	[25]
<i>Metten op proces patiëntenzorg (domein)</i>	De scope van de meting is op het domein patiëntenzorg.	[33]
<i>Metten op informatievoorziening</i>	De scope van de meting beperkt zich tot continuïteit van de informatievoorziening	
<i>Eenmalige meting</i>	Het meetinstrument wordt ingezet bij evalueren van projecten en zal dan ook in een eenmalige meting moeten kunnen voldoen.	

3.4. Samenvatting

Een beoordelingsinstrument helpt bij het bepalen of continuïteitsbeheer afdoende is geregeld. In dit onderzoek gaat het om een instrument voor het beoordelen van continuïteitsbeheer van

informatievoorziening bij kritische bedrijfsprocessen in de gezondheidszorg. Vijf bestaande instrumenten zijn in dit hoofdstuk in kaart gebracht. Ook is, vanuit de literatuur, een lijst met criteria samengesteld waaraan een beoordelingsinstrument getoetst kan worden. In het volgende hoofdstuk worden deze criteria gevalideerd bij stakeholders in het UMC Utrecht.

4. Interviews toetsing criteria beoordelingsinstrument

Om een geschikt beoordelingsinstrument voor het UMC Utrecht te vinden was het allereerst noodzakelijk om criteria te bepalen waaraan een dergelijk beoordelingsinstrument zou moeten voldoen. Hiervoor is in de literatuur gezocht naar te beoordelen inhoudelijke aspecten van Business Continuity Management. Deze zijn behandeld in hoofdstuk 2. Andere criteria voor een beoordelingsinstrument hebben betrekking op kwaliteiten van een dergelijk instrument én scoping van het beoordelingsinstrument ten aanzien van de toepassing hiervan. Deze aspecten zijn, samen met de genoemde inhoudelijke aspecten in hoofdstuk 3 in tabelvorm als ‘conceptcriteria’ uitgewerkt.

In een serie interviews zijn deze criteria getoetst bij belangrijke stakeholders in het UMC Utrecht. In dit hoofdstuk zal de opzet van deze interviews worden toegelicht, de resultaten gepresenteerd, vergezeld van een aantal opvallende quotes. De resultaten van de interviews zijn verwerkt tot een definitieve tabel met criteria voor een beoordelingsinstrument continuïteitsbeheer, waarmee het hoofdstuk wordt afgesloten.

4.1. *Opzet interviews*

Gezien het doel van de interviews – het toetsen van gevonden informatie – is gekozen voor de vorm van het ‘gedeeltelijk gestructureerde interview’. Dit interview bestaat voor een deel uit gesloten vragen met een vaste formulering, die in een vaste volgorde worden gesteld. Hiernaast is de ruimte voor een aantal open vragen. [8] Het interview bestaat uit drie delen. Eerst een aantal vragen om beeld te krijgen met bekendheid met continuïteitsbeheer. Vervolgens worden criteria voorgelegd aan de geïnterviewde en gevraagd naar volledigheid en prioriteit. Tot slot wordt gevraagd welke medewerkers in het UMC Utrecht verder bij dit onderzoek betrokken zouden moeten worden. Het interviewschema is opgenomen als bijlage 2 bij dit rapport. De interviews zijn opgenomen en door de onderzoeker nadien integraal op papier uitgewerkt. Voorafgaand aan het interview is besproken dat resultaten geanonimiseerd verwerkt worden.

De interviews zijn gehouden met diverse belanghebbenden bij continuïteitsbeheer. Vanwege het tijdsbeslag zijn hierbij niet alle soorten stakeholders, zoals beschreven in hoofdstuk 2, geïnterviewd. Wel zijn de belangrijkste rollen vertegenwoordigd. Bij de enquêtes, een volgende stap in het onderzoek, uitgewerkt in hoofdstuk 7, zijn wel alle type stakeholders meegenomen.

Er is gesproken met 9 functionarissen uit het UMC Utrecht zowel vanuit de Directie Informatie Technologie (DIT) als vanuit andere organisatieonderdelen van het UMC (divisies en directies)

Vanuit de ICT-organisatie

- Afdelingshoofd patiëntenzorg, koppelingen en bedrijfsinformatiesystemen, Directie Informatie Technologie

- Afdelingshoofd ICT-services, Directie Informatie Technologie
- Security Officer, afdeling Informatisering, Directie Informatie Technologie

Vanuit de Business

- Informatiemanager zorgverlenende divisie
- Arts/Hoogleraar
- Manager zorg
- Staf lid Raad van Bestuur, aandachtsgebied patiëntveiligheid
- Hoofd administratieve organisatie en interne controle
- Medewerker administratieve organisatie en interne controle

4.2. Resultaten

In onderstaande paragrafen zijn de belangrijkste conclusies uit de interviews, per onderdeel beschreven.

4.2.1. Continuïteitsbeheer, bekendheid en verantwoordelijkheid

In dit deel van het interview is gevraagd of de persoon bekend is met continuïteitsbeheer, hier zelf een rol of verantwoordelijkheid in heeft en wie als hoofdverantwoordelijke voor dit proces wordt gezien.

Van de 9 geïnterviewden zeggen 5 bekend te zijn met continuïteitsbeheer. De anderen hebben er wel van gehoord, maar zijn niet bekend met de term BCM of continuïteitsbeheer. Het aandachtsgebied als geheel is voor hen nog nieuw, deelaspecten zijn wel bekend. Alle gevraagden geven aan een rol of verantwoordelijkheid in continuïteitsbeheer te hebben. In bijna alle gevallen gaat het hier om een deilverantwoordelijkheid op een specifiek deelgebied, bijv. continuïteit voor ICT-infrastructuur, informatiebeveiliging of continuïteit van het bedrijfsproces zelf. Soms bestaat die rol uit bewustwording, een controlerende rol of het geven van adviezen over continuïteitseisen.

Op de vraag wie de eindverantwoordelijkheid zou moeten hebben voor het continuïteitsbeheer worden verschillende antwoorden gegeven. Bijna de helft van de ondervraagden noemt een eindverantwoordelijke rol voor de Raad van Bestuur weggelegd. Verder wordt een belangrijke rol toegekend 'aan de lijn' in de organisatie, het management en proceseigenaar. Voor wat betreft het aandachtsgebied van de informatievoorziening en ICT-continuïteit wordt de Directie Informatietechnologie als hoofdverantwoordelijke genoemd. Een aantal keer wordt in de interviews benadrukt dat er bij de verschillende actoren in het hele proces verantwoordelijkheden liggen. Een opgemerkte tekortkoming hierbij is dat deze verantwoordelijkheden niet altijd duidelijk zijn en vaak niet expliciet vastgelegd.

4.2.2. Criteria beoordelingsinstrument

Aan de geïnterviewden zijn de criteria voor een beoordelingsinstrument, zoals ook vermeld in hoofdstuk 3, voorgelegd. Aan hen is gevraagd of deze helder en logisch zijn en is gevraagd naar het belang van deze criteria. Ook is gevraagd of er nog criteria gemist werden. Op de resultaten van de interviews is een kwalitatieve analyse gedaan. De geïnterviewde groep is te klein om de resultaten kwantitatief, statistisch, te analyseren.

Wat betreft de kwaliteitscriteria (efficiëntie, objectiviteit, normerend, valide, voldoen aan regelgeving), zijn er een aantal redelijk eensluidende conclusies

- De kwaliteit 'normerend' werd door alle geïnterviewden tenminste belangrijk of zelfs zeer belangrijk gevonden. Ook in de toelichting werd duidelijk gemaakt dat het van belang is dat je na het invullen van het beoordelingsinstrument goed kan zien waar nog verbeteracties nodig zijn.
- De kwaliteiten 'efficiënt' en 'voldoen aan regelgeving' werden relatief lager (neutraal – belangrijk) gewaardeerd. Ook hier werd toegelicht waarom. Efficiëntie werd minder belangrijk gevonden, omdat het onderwerp belangrijk genoeg is om even de tijd voor te nemen. Ook wordt een beoordeling niet gezien als iets wat zeer frequent hoeft plaats te vinden, en daarom best wel iets meer tijd mag kosten. Het voldoen aan regelgeving moet geen doel op zich zijn. "het kan afleiden van de werkelijkheid als je alleen maar kijkt of je volgens de regels werkt".
- Objectiviteit en validiteit werden over het algemeen belangrijk gevonden.

Wat betreft de scoping van het meetinstrument waren er ook een aantal opvallende zaken. Zowel het 'gericht zijn op informatievoorziening' en 'meten op het niveau van het bedrijfsproces' worden het belangrijkste gevonden. Door echt op het niveau van bedrijfsproces, en bijv. niet op de hele organisatie te meten de resultaten minder abstract. Het instrument hoeft wat de geïnterviewde betreft zeker niet alleen op aspecten van patiëntenzorg te meten. Twee geïnterviewden geven expliciet aan dat het zonde zou zijn als het instrument niet bruikbaar zou zijn rondom de andere belangrijke processen van het UMC Utrecht, te weten onderzoek en onderwijs. Hoewel bij deze bedrijfsprocessen patiëntveiligheid niet direct in het geding is, kan langdurige verstoring zeker negatieve impact hebben. Denk hierbij aan grote groepen studenten of wetenschappers die verstoken zijn van voor hen essentiële informatiesystemen en –bronnen.

Een aspect welke onder de 'scoping' van het beoordelingsinstrument gerekend kan worden is de mogelijkheid om na één meting al een goed resultaat te hebben. Met andere woorden, er zijn niet persé meerdere metingen nodig om conclusies uit het instrument te kunnen trekken. Dit aspect wordt minder belangrijk gevonden. Juist het vaker meten wordt als zinvol en zelfs noodzakelijk gezien. "Eén meting is geen meting".

Over het algemeen werden de aspecten als volledig beoordeeld. Suggesties voor uitbreiding zijn:

- Aandacht voor hervatten normale werkzaamheden na een incident. Rondom continuïteitsbeheer is er veel aandacht voor de maatregelen die je moet nemen als er een verstoring is. Vergeten wordt nog wel eens dat er ook maatregelen nodig zijn om het reguliere bedrijfsproces weer op te pakken als het incident voorbij is.
- Het beoordelen of onderhoud van de continuïteitsplanning ook periodiek wordt geëvalueerd of bijgesteld.
- Het beoordelen of afspraken en verantwoordelijkheden, dus meer aspecten van organisatie van continuïteitsbeheer duidelijk zijn vastgelegd.
- Aandacht voor het gedrag van de gebruikers. Doordat gebruikers niet altijd op de juiste manier met de systemen omgaan kan dit een bedreiging voor continuïteit zijn.

4.2.3. Stakeholders continuïteitsbeheer

Aan de geïnterviewden is ook gevraagd wie er allemaal mee zouden moeten denken bij de ontwikkeling van het beoordelingsinstrument. De volgende rollen/functies zijn hierbij genoemd:

- medisch professional
- divisie management
- ICT-functionarissen, verantwoordelijk voor infrastructuur, applicatiebeheerders
- Informatievoorziening, functioneel beheerders, informatiemanagers in divisies
- verpleegkundigen
- onderzoekers
- medewerkers betrokken bij interne audit/AO-IC

4.2.4. Opvallende quotes interviews

Het interview als manier voor datacollectie heeft als aardige bijkomstigheid dat er treffende, belangrijke noties in het gesprek naar voren komen. Het zijn opmerkingen die niet altijd direct met de gestelde vraag te maken hebben, maar zeker niet onbelangrijk zijn. Een aantal opvallende quotes:

- “de uitdaging bij continuïteitsbeheer is om het zo in te richten dat helder wordt welke informatie voor de medisch professional nu écht de hoogste beschikbaarheid moet hebben. De primaire reactie is vaak, alles is belangrijk, de kunst is om er achter te komen wat nu écht 100% beschikbaar moet zijn” (*management centrale ICT-organisatie*)
- “De IT moet de spiegel van de zorg zijn. Dat betekent dus dat die systemen 24 x 7 uur paraat moeten zijn, net als de zorgverlening zelf.”... “Elke 5 minuten dat je de data later in kan voeren neemt de kwaliteit van de gegevensvastlegging ook af” (*arts*)
- “De gebruiker heeft zelf ook een verantwoordelijkheid in continuïteitsbeheer.. Die moet zelf ook nadenken wat hij kan doen als er een computer uitvalt. Misschien kan hij wel in een andere kamer verder werken. Het is een kwestie van bewustwording bij alle betrokkenen” (*informatiemanager zorgverlenende divisie*)

- “Bij uitval van kritische systemen is het niet zozeer de vraag óf maar wanneer het gaat gebeuren. We hebben bij andere ziekenhuizen ook calamiteiten en problemen gezien. Dat gaat ons dus ook een keer overkomen” (*security officer, centrale ICT-organisatie*)
- “Beoordelen van continuïteitsbeheer is ook een zaak van het evenwicht tussen vertrouwen en wantrouwen. Als een medewerker zegt dat hij het goed geregeld heeft, kunnen we daar dan vanuit gaan, of moeten we toch verder kijken?” (*stafid, aandachtsgebied patiëntveiligheid*)

4.3. Definitieve criteria beoordelingsinstrument

Op basis van de feedback verkregen uit de interviews zijn de concept criteria voor het beoordelingsinstrument aangepast.

Bij de inhoudelijke criteria is een aspect ‘Evaluatie en bijstelling continuïteitsplan’ toegevoegd. In de conceptversie was alleen sprake van bijstellen van maatregelen. Ook is er bij de inhoudelijke aspecten een kopje ‘organisatie’ toegevoegd, waaronder ‘verantwoordelijkheden en rolverdeling’ als nieuw aspect benoemd is. Verschillende geïnterviewden benadrukken het belang en in de huidige situatie het gemis, van helderheid hierover in het continuïteitsbeheer. Toegevoegd bij de maatregelen zijn maatregelen voor terugkeer naar normale bedrijfssituatie na een incident.

Eén criterium is in de definitieve versie komen te vervallen. Het gaat hier om de kwaliteit dat het instrument al resultaat geeft bij een eenmalige meting. Over het algemeen wordt het eenmalig meten niet heel sterk en zeker geen doel op zich gevonden. In tabel 2 zijn de definitieve criteria voor het beoordelingsinstrument weergegeven.

Tabel 2 Definitieve criteria beoordelingsinstrument

Criterium	Omschrijving	Bron
Inhoudelijke aspecten		
Risicoanalyse		
<i>Vaststellen bedreigingen</i>	Het benoemen van mogelijke bedreigende incidenten voor continuïteit van het betreffende bedrijfsproces	[22], [16]
<i>Vaststellen waarschijnlijkheid</i>	Het benoemen van de waarschijnlijkheid dat het bedreigende incident plaatsvindt	[23]
Business Impact Analyse		
<i>Vaststellen impact</i>	Identificeren, kwantificeren en kwalificeren van schade ontstaan door verstoring van bedrijfsproces	[13], [22]
<i>Vaststellen MUD</i>	Vaststellen maximale duur van verstoring proces	[16]
<i>Vaststellen MGv</i>	Vaststellen maximaal toelaatbaar verlies aan gegevens	[16]
Maatregelen		
<i>Vaststellen preventieve maatregelen</i>	Maatregelen ter voorkoming van verstoring of afwendend dreiging van incident	[6]
<i>Vaststellen correctieve maatregelen</i>	Maatregelen om in het geval van een incident zo snel mogelijk bedrijfsproces te kunnen hervatten en evt. schade te herstellen	[6]
<i>Vaststellen maatregelen terugkeer</i>	Maatregelen om na een incident de normale	

<i>normale bedrijfsproces</i>	bedrijfsvoering weer te continueren.	
Evaluatie		
<i>Testen maatregelen</i>	Het periodiek testen van maatregelen	[22]
<i>Onderhoud maatregelen</i>	Bijstellen van maatregelen ingebed in reguliere wijzigingsbeheerprocessen	[22]
<i>Evaluatie en bijstelling continuïteitsplan</i>	Het periodiek, op vastgestelde momenten, evalueren en bijstellen van het business continuity plan.	
Organisatie		
<i>Verantwoordelijkheden en rolverdeling</i>	Het beschrijven van rolverdeling en verantwoordelijkheden van actoren betrokken in het continuïteitsbeheer	
Criterium	Omschrijving	Bron
Kwaliteitsaspecten		
<i>Efficiëntie</i>	De juiste vragen worden gesteld, zodat meting efficiënt plaatsvindt.	[49]
<i>Objectief</i>	Onderzoeker mag geen invloed hebben op het resultaat. Meting uitgevoerd door verschillende personen moet zelfde uitslag geven.	[49]
<i>Normerend</i>	het meetinstrument moet voldoende discriminerend vermogen hebben. Het moet een meetlat zijn waardoor vergelijking tussen verschillende metingen mogelijk worden	[49]
<i>Valide</i>	De resultaten van de test zeggen daadwerkelijk iets over het gemeten onderwerp (ic continuïteitsbeheer)	[49]
<i>Voldoen aan regelgeving</i>	Wordt in het meetinstrument getoetst op de aspecten zoals die in de NEN-norm voor informatiebeveiliging (NEN7510) voor continuïteitsbeheer zijn vastgesteld? Deze norm is straks leidend bij het landelijk EPD.	[29]
Scope van meetinstrument		
<i>Metten op niveau bedrijfsproces (detailniveau)</i>	De scope van de meting is het bedrijfsproces (een BCM meting kan bijv. ook op het niveau van de organisatie als geheel plaatsvinden)	[25]
<i>Metten op proces patiëntenzorg (domein)</i>	De scope van de meting is op het domein patiëntenzorg.	[33]
<i>Metten op informatievoorziening</i>	De scope van de meting beperkt zich tot continuïteit van de informatievoorziening	

4.4. Samenvatting

De groep geïnterviewden is bekend met continuïteitsbeheer, niet altijd met de exacte concepten, maar wel met onderdelen. Allen hebben enige rol of verantwoordelijkheid in dit proces, hoewel niet altijd helder en formeel vastgelegd. Eindverantwoordelijkheid wordt gezien voor RvB, lijnmanagement en proceseigenaren en ICT-organisatie.

De voorgelegde criteria worden als volledig beoordeeld. Er wordt waarde gehecht aan het normerende karakter van een beoordelingsinstrument. Voldoen aan regelgeving wordt minder belangrijk gevonden.

Belangrijk is dat het beoordelingsinstrument op het niveau van het bedrijfsproces meet, dit hoeft niet exclusief in het domein van de patiëntenzorg te zijn, maar wel specifiek gericht op

informatievoorziening. Meegegeven wordt dat het gewenst is dat er meerdere keren gemeten wordt. Ook onderhoud van het continuïteitsplan zou periodiek moeten plaatsvinden. Op basis van deze feedback is een definitieve set criteria voor het beoordelingsinstrument ontwikkeld.

Het holistische karakter van continuïteitsbeheer komt tot uitdrukking in een diverse groep aan stakeholders, zowel uit de zorg als ICT op verschillende niveaus in de organisatie, die betrokken zouden moeten worden bij ontwikkeling van het beoordelingsinstrument.

In hoofdstuk 5 zullen de referentie beoordelingsinstrumenten gewaardeerd worden op basis van de in dit onderzoek vastgestelde criteria.

5. Beoordeling van de referentie-instrumenten

In hoofdstuk 4 is een definitieve lijst met criteria vastgesteld waaraan een beoordelingsinstrument voor continuïteitsbeheer getoetst kan worden. In dit hoofdstuk zullen de referentie-instrumenten, zoals besproken in hoofdstuk 3, beoordeeld worden. Allereerst komt de methode van het beoordelen van de instrumenten aan bod. Vervolgens in tabelvorm het uiteindelijke resultaat van de beoordeling. Na een toelichting op de beoordeling zal het hoofdstuk worden afgesloten met een conclusie.

5.1. *Methode beoordeling referentie-instrument*

Voor het beoordelen van de referentie-instrumenten zijn een aantal methoden denkbaar. Zo zou de beoordeling door een expertgroep kunnen plaatsvinden, waarbij de verschillende experts consensus bereiken over de beoordeling van ieder aspect ten aanzien van de verschillende meetinstrumenten. Dat vraagt echter een groep deskundigen die zowel bekend is met het domein van het continuïteitsbeheer en met de genoemde beoordelingsinstrumenten. Een variant hierop is het door de onderzoeker scoren van de referentie instrumenten en dit resultaat te laten valideren door een expertgroep. Een dergelijke aanpak vraagt echter een aanzienlijke resourceclaim op verschillende, veelal externe, experts, voor een beperkt deel van het onderzoek. Het gaat hierbij om een groep waarbij in dit onderzoek ook al middels interview en enquête een beroep op tijd en aandacht is gevraagd.

Er is in dit onderzoek gekozen voor de methode van het beoordelen van de referentie-instrumenten door de onderzoeker en hierbij de afwegingen zo transparant mogelijk weer te geven. Met andere woorden, per beoordeeld aspect is aangegeven onder welke condities deze als onvoldoende, voldoende of goed zijn gescoord. Het gaat dan ook niet om een objectieve of gevalideerde score, maar wel om een beoordeling die transparant en controleerbaar is.

In onderstaande tabel 3 zijn voor de verschillende aspecten de afwegingen voor beoordeling vastgelegd. Onder de tabel staat voor een aantal aspecten een nadere inhoudelijke toelichting.

Tabel 3 Scoringscriteria beoordelingsinstrumenten

	Onvoldoende -	Voldoende +	Goed ++
Inhoudelijke aspecten			
Risicoanalyse			
Vaststellen bedreigingen	Geen vraag rondom vaststellen bedreigingen	Tenminste één vraag over vaststellen bedreigingen	Meerdere vragen over vaststellen bedreigingen waarbij specifiek aandacht voor methode en procedure van risicoanalyse

<i>Vaststellen waarschijnlijkheid</i>	Geen vraag rondom vaststellen waarschijnlijkheid	Tenminste één vraag over vaststellen waarschijnlijkheid	Meerdere vragen over vaststellen waarschijnlijkheid en specifiek over vaststellen in meetbare termen
Business Impact Analyse			
<i>Vaststellen impact</i>	Geen vraag rondom vaststellen van impact	Tenminste één vraag over vaststellen impact	Meerdere vragen over vaststellen impact en specifiek over vaststellen in meetbare termen
<i>Vaststellen MUD</i>	Geen vraag rondom het vaststellen van MUD (of equivalent MTPD, Maximum Tolerable Period of Disruption)	Tenminste één vraag over vaststellen MUD (of MTPD)	Meerdere vragen over vaststellen MUD (of MTPD)
<i>Vaststellen MGv</i>	Geen vraag rondom het vaststellen van MGv (of equivalenten RPO, Recovery Point Objective of RTO, Recovery Time Objective)	Tenminste één vraag over vaststellen MGv (of RPO of RTO)	Meerdere vragen over vaststellen MGv (of RPO of RTO)
Maatregelen			
<i>Vaststellen preventieve maatregelen</i>	Geen vraag over vaststellen preventieve maatregelen (of equivalent detectie)	Tenminste één vraag over vaststellen preventieve maatregelen (of detectie)	Meerdere vragen over preventieve maatregelen, waarbij specifiek aandacht voor detectie, backup en uitwijk
<i>Vaststellen correctieve maatregelen</i>	Geen vraag over vaststellen correctieve maatregelen (of equivalent repressie)	Tenminste één vraag over vaststellen correctieve maatregelen (of repressie)	Meerdere vragen over correctieve maatregelen, waarbij specifiek aandacht voor noodprocedures.
<i>Vaststellen maatregelen terugkeer normale bedrijfsproces</i>	Geen vraag over vaststellen herstel naar normale situatie	Tenminste één vraag over vaststellen herstel naar normale situatie	Meerdere vragen over herstel naar normale situatie.
Evaluatie			
<i>Testen maatregelen</i>	Geen vraag over testen maatregelen	Tenminste één vraag over testen maatregelen	Meerdere vragen over testen maatregelen waarbij specifiek aandacht voor testprocedure en testplanning
<i>Onderhoud maatregelen</i>	Geen vraag over onderhoud maatregelen	Tenminste één vraag over onderhoud maatregelen	Meerdere vragen over onderhoud maatregelen, waarbij specifiek aandacht voor relatie met wijziging in omgeving
<i>Evaluatie en bijstelling continuïteitsplan</i>	Geen vraag over evaluatie en bijstelling continuïteitsplan	Tenminste één vraag over evaluatie en bijstelling continuïteitsplan	Meerdere vragen over evaluatie en bijstelling waarbij aandacht voor planning van onderhoud
Organisatie			
<i>Verantwoordelijkheden en rolverdeling</i>	Geen vraag over verantwoordelijkheden en rolverdeling	Tenminste één vraag over verantwoordelijkheden en rolverdeling	Meerdere vragen over verantwoordelijkheden en rolverdeling waarbij aandacht voor eindverantwoordelijkheid en coördinatie rol.
Kwaliteitsaspecten			
<i>Efficiëntie</i>	>100 vragen	50 – 100 vragen	< 50 vragen
<i>Objectief</i>	Geen toelichting bij antwoordmogelijkheden / alleen vrije tekst	Afgebakende abstracte antwoordmogelijkheden, zonder verdere instructie	Afgebakende concrete antwoordmogelijkheden
<i>Normerend</i>	Het instrument toont op geen enkele wijze of uitslag goed of slecht is	Het instrument toont in z'n algemeenheid of uitslag goed of slecht is	Het instrument toont op deelgebieden of uitslag goed of slecht is

<i>Valide</i>	Van de vragen gaat meer dan de helft niet over de inhoudelijke aspecten van continuïteitsbeheer	Van de vragen gaat minder dan de helft niet over inhoudelijke aspecten van continuïteitsbeheer	Alle vragen hebben betrekking op inhoudelijke aspecten van continuïteitsbeheer
<i>Voldoen aan regelgeving</i>	Instrument refereert niet aan nationale of internationale standaard/norm	Instrument refereert aan nationale of internationale standaard/norm	Instrument volgt structuur en alle deelgebieden van nationale of internationale standaard/norm
Scope van meetinstrument			
<i>Metten op niveau bedrijfsproces (detailniveau)</i>	Minder dan de helft van de vragen gaan over continuïteitsbeheer bedrijfsproces	Meer dan de helft van de vragen gaan over continuïteitsbeheer bedrijfsproces	Alle vragen hebben betrekking op continuïteitsbeheer bedrijfsproces
<i>Metten op proces patiëntenzorg (domein)</i>	Er komen geen patiëntenzorggerelateerde onderwerpen (zoals patiëntveiligheid) aan bod	Er wordt één of meerdere patiëntenzorggerelateerde onderwerpen genoemd	Meer dan de helft van de vragen zijn specifiek gericht op patiëntenzorg processen
<i>Metten op informatievoorziening</i>	Minder dan de helft van de vragen heeft betrekking op continuïteit van de informatievoorziening	Meer dan de helft van de vragen heeft betrekking op continuïteit van de informatievoorziening	Alle vragen hebben betrekking op continuïteit van informatievoorziening

5.1.1. Toelichting bij scoringscriteria

Bij het bepalen van de criteria wanneer een aspect onvoldoende, voldoende of goed scoort, is bij de inhoudelijke aspecten gebruik gemaakt van de theorie, zoals in hoofdstuk 2 besproken is.

Voor een aantal van de 'kwaliteitsaspecten', is geen theoretische basis beschikbaar om deze keuze op te maken. Waar mogelijk is hier wel gebruik van gemaakt. Zo is efficiëntie van het meetinstrument lastig te toetsen. In een boek over 'safety management audits' noemt Dominic Cooper 100 vragen als maximum voor een vragenlijst, omdat deze anders teveel tijd in beslag gaat nemen. [50]

Ook het criterium 'objectiviteit' is lastig SMART te maken. Tom Bakker bespreekt in zijn artikel over BCM een audit-tool. Deze tool welke uitsluitend met percentages werkt, zou makkelijk subjectief kunnen worden ingevuld. [46] Een omschrijving van categorieën in plaats van percentages maakt het beter mogelijk om objectief in te vullen. Dit uitgangspunt is verwerkt in de beoordeling hoe objectief de tool kan worden ingevuld. Naarmate de antwoordmogelijkheden concreter omschreven zijn, is de kans groter dat dit op een eenduidige manier wordt ingevuld.

Voor wat betreft het aansluiten bij regelgeving is de volgende indeling gehanteerd.

Beoordelingsinstrumenten die geen verwijzing kennen naar een bijbehorende norm of standaard.

Beoordelingsinstrumenten die expliciet, in naamgeving of omschrijving, horen bij een norm of standaard. Tot slot de beoordelingsinstrumenten die een norm of standaard volledig volgen en ook de hoofdstukindeling of alle aspecten van de betreffende norm behandelen.

5.2. Resultaat beoordeling referentie-instrumenten

In onderstaande tabel 4 is het resultaat van de beoordeling van de verschillende instrumenten opgenomen. De score heeft per aspect plaatsgevonden waarbij '-' staat voor onvoldoende, '+' voor voldoende en '++' voor goed. De laatste rij van de tabel geeft de totaalscore weer. Deze totaalscore is

de gemiddelde score van alle aspecten, waarbij ieder aspect gelijk 'gewogen' is. Onder tabel 4 volgt voor ieder instrument nog een nadere toelichting, welke zich niet in de scoringstabel laat uitdrukken.

Tabel 4 Beoordeling referentie-instrumenten

	Monitor Informatie- beveiliging <i>Hoofdstuk 9</i>	NEN7510 Checklist Continuïteits- planning	BCMM	BCI PAS56 Audit Workbook	Code voor informatie- beveiliging
Inhoudelijke aspecten					
Risicoanalyse					
Vaststellen bedreigingen	+	-	-	++	++
Vaststellen waarschijnlijkheid	-	-	-	+	-
Business Impact Analyse					
Vaststellen impact	+	-	-	++	++
Vaststellen MUD	+	-	-	+	++
Vaststellen MGv	+	-	-	++	-
Maatregelen					
Vaststellen preventieve maatregelen	+	+	-	+	++
Vaststellen correctieve maatregelen	++	+	-	+	++
Vaststellen maatregelen terugkeer normale bedrijfsproces	+	+	-	+	++
Evaluatie					
Testen maatregelen	++	++	-	++	++
Onderhoud maatregelen	+	-	+	++	++
Evaluatie en bijstelling continuïteitsplan	++	-	+	++	++
Organisatie					
Verantwoordelijkheden en rolverdeling	++	++	-	++	++
Kwaliteitsaspecten					
Efficiëntie	++	++	++	-	+
Objectief	++	++	++	+	++
Normerend	+	-	++	++	-
Valide	++	++	+	++	++
Voldoen aan regelgeving	++	++	-	++	++
Scope van meetinstrument					
Metten op niveau bedrijfsproces (detailniveau)	+	++	-	-	+
Metten op proces patiëntenzorg (domein)	-	-	-	-	-
Metten op informatievoorziening	++	++	-	-	++
Totaal score	+	+	-	+	++

5.2.1. Toelichting bij resultaat

De totaal score van de 5 instrumenten laat zien dat één instrument onvoldoende is, drie voldoende en één goed. Per instrument zal een korte toelichting bij de score worden gegeven.

Hoofdstuk 9 van de *Monitor informatiebeveiliging* [40] laat bijna alle inhoudelijke aspecten aan bod komen, zij het oppervlakkig. Het is dan ook een korte vragenlijst die zich relatief snel laat invullen. De presentatie van de resultaten is nogal beperkt voor het onderdeel continuïteitsbeheer. Aangezien dit één van de 11 hoofdstukken van de monitor – en tevens van NEN 7510 - is, wordt continuïteitsbeheer als deelonderwerp niet verder gedifferentieerd.

Ook de *checklist continuïteitsplanning NEN7510* [25] die onderdeel vormt van het handboek NEN7510 is een relatief korte vragenlijst. Naast de gesloten antwoordmogelijkheden is er ruimte voor toelichting bij de antwoorden. Dit is ook het geval bij de *PAS56 Audit Workbook*. De checklist behandelt slechts een deel van de inhoudelijke aspecten. Ook een echte eindscore of normering ontbreekt.

De *BCMM survey* [48] schiet in de beoordeling aan veel kanten te kort. Deze korte vragenlijst richt zich alleen op algemene, organisatiebrede aspecten van continuïteitsbeheer. Deze online survey heeft wel een directe terugkoppeling in normering door middel van een volwassenheidsniveau.

De *BCI PAS56 Audit Workbook* [43] is met afstand de meest uitgebreide en gedetailleerde checklist. Ook deze richt zich in vooral op het niveau van de organisatie en scoort daarom op een aantal inhoudelijke, meer op bedrijfsproces gerichte, aspecten 'slechts' voldoende. Er is veel aandacht voor de organisatie van continuïteitsbeheer en een duidelijke, gedetailleerde terugkoppeling middels een radardiagram. Dit instrument is opgenomen in een Excel spreadsheet en maakt op transparante wijze gebruik van wegingsfactoren en formules. Hierdoor is inzichtelijk hoe de uiteindelijke score tot stand is gekomen.

De checklist bij de *Code voor informatiebeveiliging* [42] is het enige instrument welke in de totaal score op 'goed' uitkomt. Op bijna alle inhoudelijke aspecten wordt gedetailleerd doorgevraagd. Belangrijkste mindere punten; het invullen van het instrument vertaalt zich niet in een 'waardering' en het aantal vragen is aan de hoge kant.

Geen van de instrumenten besteedt specifieke aandacht aan het domein patiëntenzorg, ook niet de twee instrumenten die gebaseerd zijn op NEN7510, de norm voor informatiebeveiliging in de gezondheidszorg.

Bij het beoordelen van de instrumenten komen ook nieuwe eigenschappen naar voren, die weliswaar niet eerder expliciet waren vastgesteld, maar zeker relevant kunnen zijn:

- Enkele instrumenten geven de ruimte voor toelichting in vrije tekst bij de gecodeerde antwoordmogelijkheden
- Van de vijf instrumenten zijn er drie Nederlandstalig. Dit lijkt een voordeel. In de Nederlandse ziekenhuizen is Nederlands de voertaal, ook voor bijvoorbeeld protocollen en procedures

- De PAS56 Audit Workbook maakt gebruik van een weging per vraag. Dit biedt een mogelijkheid om minder belangrijke en belangrijke aspecten verschillend mee te laten tellen in de uiteindelijke beoordeling.

5.3. *Samenvatting*

Van de vijf beoordeelde instrumenten wordt de checklist van *code voor informatiebeveiliging* als enige als goed beoordeeld. Inhoudelijk worden de meeste aspecten goed afgedekt. Echter de beoordeling laat ook zien dat deze checklist op een aantal deelaspecten beter kan. Zo mist uiteindelijk een normering behorende bij de verschillende van continuïteitsbeheer en is de vragenlijst nogal omvangrijk. Niet in de beoordeling meegenomen, maar wel opvallend is het feit dat een aantal van de beoordelingsinstrumenten naast gesloten antwoordmogelijkheden, ook ruimte bieden voor toelichting. Dit lijkt een zinvolle mogelijkheid om mee te nemen in een beoordelingsinstrument. De score van het continuïteitsbeheer laat zich op die manier ook beter interpreteren en echt op waarde inschatten.

De instrumenten hebben ieder eigen sterke punten. In een nieuw beoordelingsinstrument voor continuïteitsbeheer kan een aantal van deze kwaliteiten worden gecombineerd. Hoofdstuk 6 behandelt dit nieuwe beoordelingsinstrument.

6. Een nieuw beoordelingsinstrument

In hoofdstuk 5 zijn een vijftal referentie-instrumenten beoordeeld. Deze instrumenten voldoen in verschillende mate aan de gestelde criteria. Daarnaast is ook duidelijk geworden dat de verschillende instrumenten ieder hun sterke en mindere kanten kennen. Waar bij het ene instrument bijvoorbeeld alle inhoudelijke aspecten van het continuïteitsbeheer worden getoetst, is het andere instrument weer sterker in het presenteren van een 'norm' rondom continuïteitsbeheer. In dit hoofdstuk komt de ontwikkeling van een nieuw beoordelingsinstrument continuïteitsbeheer aan bod. Aan de hand van de criteria uit hoofdstuk 4, zullen de keuzes worden toegelicht bij de ontwikkeling van het nieuwe instrument. Ook wordt duidelijk gemaakt hoe hierin de bestaande instrumenten zijn gebruikt.

6.1. *Methode van ontwikkeling*

Bij het ontwikkelen van een nieuw instrument zijn op basis van de bestaande instrumenten de beste kwaliteiten van de verschillende instrumenten gecombineerd. Hierbij is ook kritisch gekeken naar aspecten die in tegenspraak met elkaar kunnen zijn. Het PAS56 Audit Workbook [43] bijvoorbeeld kenmerkt zich door zeer uitgebreid aan alle inhoudelijke aspecten aandacht te besteden, maar is met de 186 vragen ook een zeer uitgebreide en daarmee minder efficiënte vragenlijst. Bij het nieuwe instrument is deze efficiëntie bereikt door bijvoorbeeld vragen over continuïteitsbeheer op het niveau van de totale organisatie/instelling weg te laten. De scoping van het beoordelingsinstrument, zoals ook benadrukt in de criteria in hoofdstuk 4, beperkt zich tot het continuïteitsbeheer rondom het bedrijfsproces.

Om tot een mix en match te komen van de verschillende kwaliteiten, zijn de volgende keuzes gemaakt:

- Een belangrijk deel van de vragen is gebaseerd op de *checklist code voor informatiebeveiliging* [42]. In deze checklist zijn Nederlandstalige vragen van voldoende detailniveau, ten aanzien van de inhoudelijke criteria. Ook is de antwoordmogelijkheid 'ja', 'nee', 'gedeeltelijk' en 'onbekend' behouden. Waar vragen ontbreken, bijvoorbeeld met betrekking tot risico- en business analyse zijn ofwel vragen uit andere instrumenten gebruikt ofwel zijn deze door de onderzoeker zelf geformuleerd.
- Er is mogelijkheid geboden om vrije tekst toe te voegen aan de gestructureerde antwoordmogelijkheden, zodat een antwoord als 'gedeeltelijk' of 'ja' inhoudelijk beter geïnterpreteerd kan worden.
- Voor de technische vormgeving van het beoordelingsinstrument is gekeken naar het PAS56 Audit Workbook [43]. Het gaat hier om de keuze voor een excelsheet met per tabblad vragen over één aspect. Per vraag is er de mogelijkheid om een wegingsfactor mee te nemen én een uiteindelijke presentatie van de resultaten in een Radar diagram. Op deze manier ontstaat een

interactief beoordelingsinstrument die direct en in één oogopslag grafisch de resultaten kan tonen.

- In het PAS56 Audit Workbook worden de resultaten per deelgebied uitgedrukt in een percentage en middels een kleurcodering wordt er een impliciete waardering aan gegeven. Tussen 95% en 100% is dit groen, 80% - 84% is geel, percentages hieronder zijn rood. Deze analogie met een stoplicht is overgenomen in het nieuwe beoordelingsinstrument.

6.2. Opzet nieuw beoordelingsinstrument

Zoals aangegeven is het nieuwe beoordelingsinstrument gebaseerd op eigenschappen van de getoetste bestaande instrumenten. In de volgende paragrafen komt de opzet van het instrument gedetailleerd aan bod. Hierbij worden de thema's indeling, antwoordmogelijkheden, score, weging en presentatie van het nieuwe instrument behandeld.

6.2.1. Indeling

Bij de indeling van het beoordelingsinstrument wordt onderscheid gemaakt tussen de implementatie (vorm) en de inhoud.

Voor de implementatie van het nieuwe beoordelingsinstrument is gekozen voor een Excel werkmap welke in 7 tabbladen is onderverdeeld. In totaal bevat het 48 vragen, allen uniek gecodeerd aan de hand van conventie "tabbladnummer.vraagnummer". Deze implementatie is op hoofdlijnen gelijk aan die van de PAS 56 Audit Workbook. [43]

Het eerste tabblad, genaamd 'algemene gegevens', biedt ruimte om identificerende gegevens rondom de beoordeling en het proces vast te leggen (tabel 5).

Tabel 5 Algemene gegevens

1.0	Naam bedrijfsproces
1.1	Datum beoordeling
1.2	Beoordeling door (naam)
1.3	Beoordeling door (functie)
1.4	Naam proceseigenaar
1.5	Functie proceseigenaar

Daarnaast is op het eerste tabblad algemene informatie aanwezig over het beoordelingsinstrument, versienummer, totstandkoming en korte werkinstructie.

In de tabbladen 2 t/m 6 zijn de vragen opgenomen welke de daadwerkelijke input vormen voor beoordeling van het continuïteitsbeheer. De tabbladen zijn ingedeeld naar inhoudelijke aspecten die in hoofdstuk 2 en hoofdstuk 4 zijn vastgesteld.

- Organisatie
- Risico- en Impactanalyse
- Maatregelen
- Testen
- Onderhoud

Bij de volgorde van de tabbladen, en daarmee ook de vraagvolgorde, is het proces van het continuïteitsbeheer als leidend principe gebruikt. Als eerste is het proces overstijgende aspect 'organisatie' geplaatst. Deze keuze is gemaakt aangezien er bij 'organisatie' een aantal vragen worden gesteld, waarop bij andere aspecten voortgebouwd wordt. Het gaat hierbij bijvoorbeeld om een vraag als 'Is er een continuïteitsplan?'. Bij het onderdeel 'onderhoud' wordt in detail doorgevraagd over het continuïteitsplan.

De tabbladen zijn gelijkvormig van opbouw. Achter iedere vraag is middels een 'picklist' keuze te maken uit de antwoordmogelijkheden 'Ja', 'Nee', 'Gedeeltelijk' en 'Onbekend'. In de volgende paragraaf wordt verder ingegaan op de keuze hiervoor. Achter dit antwoord is ruimte voor een toelichting bij het antwoord in vrije tekst. In de drie kolommen achter het antwoord worden automatisch scores berekend, ook deze komen in de volgende paragraaf verder aan bod. Onder aan het tabblad wordt de gemiddelde score (een percentage tussen 0 en 100%) van de betreffende categorie weergegeven.

6.2.2. Antwoordmogelijkheden

Bij de keuze van het type antwoordmogelijkheden speelt een dilemma. Om dit toe te lichten is een korte introductie op het gebied van meten en statistiek nodig.

Dirk Speelman legt in zijn introductie in statistiek de verschillen tussen meetniveaus uit. [51] Bij nominale variabelen is geen enkele rekenkundige vergelijking mogelijk. Denk hierbij aan bijvoorbeeld provincies (Utrecht, Groningen etc.). Bij ordinale variabelen is wel sprake van een ordening, maar is de afstand tussen de verschillende niet absoluut en daarmee verschillend interpreteerbaar (onvoldoende, voldoende, goed, zeer goed). Dit is wel het geval bij een intervallschaal. Daar is niet alleen sprake van een ordening, maar heeft ook de afstand tussen de verschillende waarden betekenis. Denk hierbij aan *graden Celsius*. Daarmee is ook het rekenen met ordinale variabelen feitelijk onjuist. Van de onderzochte beoordelingsinstrumenten werkt alleen het BCI PAS56 Audit Workbook [43] met een intervallschaal. De antwoorden dienen gegeven te worden in percentages. Bij de bespreking van dit instrument, in paragraaf 3.2.4. werd al geconstateerd dat dergelijke percentages lastig te interpreteren zijn. Hoewel er dus sprake is van een intervallschaal waarmee goed te rekenen, is het tegelijkertijd de vraag hoeveel waarde is toe te kennen aan het resultaat. De andere onderzochte beoordelingsinstrumenten kennen ordinale schalen, de meesten met de antwoordmogelijkheden 'Ja', 'Nee', 'Gedeeltelijk'.

Voor de sociale wetenschappen zijn technieken ontwikkeld waarmee ordinale waarden 'vertaald' kunnen worden naar intervalschalen, zoals die van Rasch of Thurstone. [52] Dit onderzoek kent geen uitgebreide zoektocht naar schalings methoden die deze ordinale schaal in een interval schaal zouden kunnen vertalen. Pelsmaecker heeft het in zijn boek over marktonderzoek over de veel gebruikte methode van 'de arbitraire schaal', waarbij de onderzoeker zelf op basis van behoeften en inzichten een schaal creëert. [53] Bij het nieuwe beoordelingsinstrument is gekozen voor de indeling 'Ja', 'Nee', 'Gedeeltelijk' en 'Onbekend', welke voor de invuller herkenbare keuzes representeren. Tegelijkertijd is aan deze antwoordmogelijkheden een percentage toegekend, zodat deze gebruikt kan worden bij het berekenen van gemiddelde scores. In tabel 6 staan de antwoordmogelijkheden en bijbehorende score opgenomen.

Tabel 6 Antwoordmogelijkheden beoordelingsinstrument

Antwoordmogelijkheden	Score
Ja	100%
Gedeeltelijk	50%
Nee	0%
Onbekend	0%

6.2.3. Weging en berekening score

Voor de berekening van scores op zowel deelaspecten als totaal is hetzelfde mechanisme als in de BCI PAS56 Audit Workbook is gebruikt. De andere beoordelingsmodellen kenden geen toegankelijke en transparante vertaling van uitkomsten van de checklists naar het eindresultaat. In figuur 10 is een fragment van het beoordelingsinstrument opgenomen, waarin inzichtelijk wordt hoe de score per vraag tot stand komt. Bij de antwoorden is een percentage ingevuld, iedere vraag kent een wegingsfactor, welke uiteindelijk in een gewogen score resulteert.

LIFE CYCLE STAGE	NO. OF QUESTIONS	QUESTION NO.	QUESTIONS	TOTAL NO. OF RETUR	ANSWERS								AVERAGE SCORE	QUESTION WEIGHT	WEIGHTED SCORE	COMPLIANCE
					NO (0%)	20%	40%	60%	80%	90%	YES (100%)	N/A				
Each Stage Section Aggregate Dashboard.																
	1	1	Organisation (Corporate) BCM Strategy	1	0	0	0	0	1	0	0	0	80	1,00	80	80
	1	2	Process Level (Systemic) BCM Strategy	1	0	0	0	0	1	0	0	0	80	1,00	80	80
	1	3	Resource Recovery BCM Strategy.	1	0	0	0	1	0	0	0	0	60	1,00	60	60

Figuur 10 Scoreberekening BCI PAS56 Audit Workbook

Ditzelfde principe is ook op het nieuwe beoordelingsinstrument toegepast. Eerder kwam al de percentages aan bod, corresponderend met de verschillende antwoordmogelijkheden. In figuur 11 is de scoreberekening in het nieuwe beoordelingsinstrument afgebeeld.

Vraagnr	Vraag	Antwoord	Opmerkingen	Score	Gewicht	Gewogen score
4.11	Is vastgelegd wie verantwoordelijk is voor uitvoering van uitwijk- of failoverprocedure?	Gedeeltelijk		50	1	50
4.12	Is een zogenaamde 'uitwijkkoffer' beschikbaar waarin (kopieën van) uitwijk- en terugkeerprocedures veilig bewaard kunnen worden?	Ja		100	1	100
4.13	Zijn afspraken met externe leveranciers gemaakt rondom reparatie, reserveonderdelen etc?	Ja		100	1	100
Maatregelen tbv hervatten werkzaamheden						
4.14	Is er een terugkeerprocedure waarin wordt beschreven welke acties dienen te worden ondernomen om de normale bedrijfsvoering te hervatten?	Ja		100	0,5	50

Figuur 11 Scoreberekening nieuw beoordelingsinstrument

Per aspect en dus ook per tabblad in het beoordelingsinstrument wordt een eindscore berekend. In deze berekening wordt de som van de gewogen scores gedeeld door de som van de gewichten. Bij het nieuwe beoordelingsinstrument is zeer beperkt gebruik gemaakt in differentiatie door weging. Bijna alle vragen hebben een wegingsfactor 1 meegekregen.

In het Audit Workbook is standaard de wegingsfactor bij iedere vraag zo ingericht dat alle antwoorden gelijkwaardig meewegen. Als argument hiervoor is gegeven dat het voldoen aan ieder aspect uit het 'workbook' feitelijk verplicht is. Niettemin wordt ook erkend dat de aard van de organisatie van invloed kan zijn op het daadwerkelijke gewicht welke de verschillende vragen hebben. Daarom biedt het instrument ruimte om de wegingsfactoren aan te passen. [43]

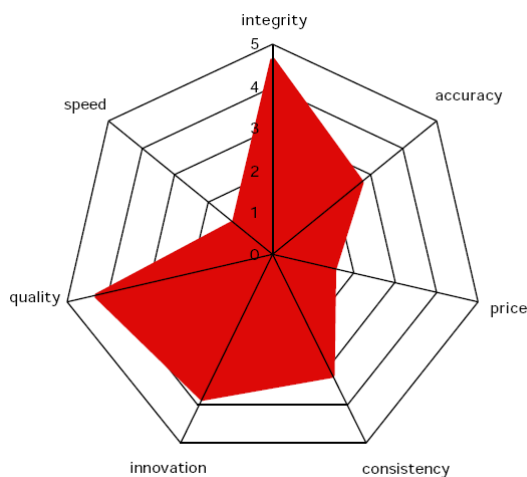
Het bepalen van het gewicht van de verschillende vragen vraagt ervaring en praktijkresultaten bij het gebruik van het nieuwe beoordelingsinstrument. Dit valt buiten de scope en doorlooptijd van dit onderzoek. Voor een beperkt aantal vragen heeft de onderzoeker er echter voor gekozen een afwijkende wegingsfactor van 0,5 te kiezen. Het gaat hierbij om deelaspecten die in de waarneming van de onderzoeker nog nauwelijks in praktijk in het continuïteitsbeheer in het ziekenhuis zijn ingeregeld. Het effect van deze weging is in dit onderzoek niet verder gevalideerd om eerder genoemde reden van scoping en doorlooptijd. In tabel 7 zijn de vragen genoemd die deze wegingsfactor hebben meegekregen.

Tabel 7 Vragen met wegingsfactor 0,5

3.3	Is vastgesteld hoe waarschijnlijk het optreden van de genoemde risico's is?
4.9	Is er een systeem van nood-accounts en procedures voor de inzet van deze nood-accounts? (zodat bij problemen met gebruikers accounts, er beheerst noodaccounts uitgereikt kunnen worden)
4.14	Is er een terugkeerprocedure waarin wordt beschreven welke acties dienen te worden ondernomen om de normale bedrijfsvoering te hervatten?

6.2.4. Presentatie resultaten

Voor het presenteren van de scores is gebruik gemaakt van een radardiagram, ook wel spin- of sterdiagram genoemd. Deze vorm van presenteren, zoals afgebeeld in figuur 12, is ook gebruik bij het presenteren van de resultaten van de Monitor Informatiebeveiliging [40] en de BCI PAS56 Audit Workbook [43]. In een beschrijving van de “University of California” wordt als eigenschap van dit type diagram genoemd dat het van verschillende performancecategorieën de sterkte en zwakten toont. [54] Het is juist deze kwaliteit die gebruikt wordt om inzicht te geven in de status van het continuïteitsbeheer op verschillende deelaspecten.



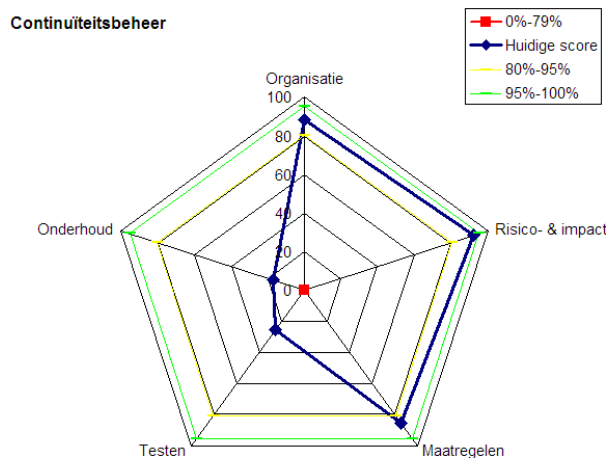
Figuur 12 Voorbeeld van een radardiagram [54]

Het radardiagram kent als ‘spaken’ de categorieën waar in de verschillende tabbladen op gescoord is te weten:

- Organisatie
- Risico- en Impactanalyse
- Maatregelen
- Testen
- Onderhoud

De gemiddelde score per categorie kent een waarde tussen de 0 en 100%. De vertaling van een percentage naar een waardeoordeel vraagt een verdere validatie van de scores, welke geen onderdeel uitmaakt van dit onderzoek. Indicatief is de eerder besproken indeling van het PAS56 Audit Workbook overgenomen. De kleurcodering wordt gebruikt, zonder aan deze kleuren een direct waardeoordeel (goed, onvoldoende etc.) te koppelen.

In het diagram zijn referentie lijnen opgenomen bij 0% (rood), 80% (geel) en 95% (groen). In één oogopslag is met dit diagram zichtbaar in welke categorieën hoog of laag is gescoord. Zie hiervoor ook het voorbeeld in figuur 13.



Figuur 13 Radardiagram nieuw beoordelingsinstrument

6.3. Samenvatting

Op basis van de kwaliteiten van de verschillende referentie-beoordelingsinstrumenten is een nieuw beoordelingsinstrument ontwikkeld. Het nieuwe beoordelingsinstrument is vormgegeven in een Excel spreadsheet met 48 Nederlandstalige vragen. Per tabblad staan vragen over een bepaald aspect van continuïteitsbeheer. Als antwoordmogelijkheid zijn middels een keuzelijst de antwoorden 'ja', 'nee', 'gedeeltelijk' en onbekend beschikbaar en is ruimte voor toelichting. De berekende resultaten worden weergegeven in een radardiagram.

Hoofdstuk 7 is gewijd aan de validatie van dit nieuwe instrument. Enerzijds is hierbij middels een enquête het oordeel van belangrijke stakeholders gevraagd, anderzijds is het instrument toegepast in een praktijkcase.

7. Validatie beoordelingsinstrument

In het vorige hoofdstuk is een nieuw beoordelingsinstrument continuïteitsbeheer gepresenteerd. Deze is ontwikkeld op basis van bestaande instrumenten én criteria waaraan een beoordelingsinstrument zou moeten voldoen. De volgende stap in het onderzoek is het valideren van dit nieuwe beoordelingsinstrument. Hiervoor zijn twee methodes gebruikt. Allereerst is in een schriftelijke enquête bij de belangrijkste belanghebbenden in het UMC Utrecht het oordeel gevraagd over het nieuwe beoordelingsinstrument. Deze enquête is ook voorgelegd aan stakeholders in twee andere UMC's. Daarnaast is het nieuwe instrument gebruikt om in een echte praktijk case toe te passen. Achtereenvolgens zullen van beide methoden de werkwijze en resultaten worden toegelicht.

7.1. Aanpak enquête

Om het beoordelingsinstrument te toetsen bij de belanghebbenden is gekozen voor de vorm van enquête. In tegenstelling tot de interviews kon nu een grotere groep betrokken worden in het onderzoek. De enquêtes zijn via email verstuurd. In deze email is zowel de vragenlijst, als word-bestand en het beoordelingsinstrument als Excel-bestand bijgevoegd. De enquête, opgenomen als bijlage 4, bestaat uit 7 open vragen.

Voordat de enquête verstuurd is, is eerst met drie personen een zogenaamde 'pilot test' gedaan. In interviewvorm zijn de vragen doorgenomen, zodat op deze manier een validatie van de vragenlijst kon plaatsvinden.

De enquête is verstuurd naar de belanghebbenden zoals deze in hoofdstuk 2, vanuit de literatuur zijn geïdentificeerd en naar aanleiding van aanvullingen hierop uit de interviews, zoals besproken in hoofdstuk 4. Naast medewerkers van het UMC Utrecht is de enquête verstuurd aan security officers van het Leids Universitair Medisch Centrum (LUMC) en het Rotterdamse Erasmus Medisch Centrum. Het onderwerp continuïteitsbeheer rondom informatievoorziening is normaliter belegd bij deze functionarissen. In de email is evenwel vermeld dat deze ook doorgestuurd kon worden naar een andere functionaris, als deze grotere betrokkenheid bij het onderwerp zou hebben. In totaal hebben 17 personen deelgenomen aan de enquête welke aan 19 personen was verstuurd, waarmee de response rate op 89% komt.

In tabel 8 staan de functies van de geënquêteerden genoemd en de respons. Net als bij de interviews zijn ook de enquêtes anoniem verwerkt.

Tabel 8 Respondenten enquête

Organisatie (onderdeel)	Functie	Respons + bijzonderheden
UMC Utrecht		
Divisie Heelkundige Specialismen	Manager bedrijfsvoering	Ja
Divisie Heelkundige specialismen	Hoogleraar / Medisch Specialist	Nee

Divisie Hart & Longen	Manager Zorg	Ja
Divisie Hart & Longen	Verpleegkundig specialist	Ja
Divisie Hersenen	Informatiemanager	Ja
Divisie Int. Geneeskunde Dermatologie	Projectleider Elektronisch Patiënten Dossier (EPD)	Ja
Divisie Int. Geneeskunde Dermatologie	Informatiemanager	Ja
Directie Informatie Technologie	Projectleider Elektronisch Patiënten Dossier (EPD)	Ja
Directie Informatie Technologie	Afdelingshoofd Patiëntenzorgsystemen	Ja
Directie Informatie Technologie	Afdelingshoofd ICT-services	Ja, interview
Directie Informatie Technologie	Security officer	Ja
Directie Informatie Technologie	Beheerder EPD	Ja
Directie Informatievz & Financiën	Hoofd Zorgadministratie & Systemen	Nee, overgedragen aan medewerker
Directie Informatievz & Financiën	Functioneel applicatiebeheerder	Ja
Directie Informatievz & Financiën	Hoofd AO/IC	Ja, interview
Directie Informatievz & Financiën	Medewerker AO/IC aandachtsgebied EDP	Ja, interview
Raad van Bestuur	Staflid, aandachtsgebied patiëntveiligheid	Ja, interview
LUMC	Specialist informatiebeveiliging	Ja
Erasmus MC	Security officer	Ja

7.2. Resultaten enquête

Gezien de vorm van de enquête, open vragen, en de beperkte groep van 17 respondenten zijn de resultaten niet statistisch verwerkt. In deze paragraaf volgt een kwalitatieve analyse van de resultaten. De enquêtes zijn bijna allemaal volledig ingevuld. Twee respondenten hebben vraag 5 t/m 7 niet ingevuld, waarschijnlijk zijn deze over het hoofd gezien omdat ze op de tweede pagina van het toegestuurde word-document stonden. Eén respondent heeft naast de vragenlijst ook het beoordelingsinstrument ingevuld. Aangezien dit niet het doel of de vraag van dit onderzoek was, is het ingevulde beoordelingsinstrument bij de verwerking buiten beschouwing gelaten. Bij de personen waarbij in interview vorm de enquête is doorgenomen valt op dat er uitgebreidere en meer gedetailleerde antwoorden op de vragen zijn gegeven. Wellicht heeft dit te maken met het interactieve karakter van de interviewvorm. In zijn 'research methods knowledge base' beschrijft Trochim het deze mogelijkheid van 'doorvragen' in de interview-setting ten opzichte van de 'questionnaire'. [55] Ook de specialisten op het gebied van informatiebeveiliging, zowel uit het UMC Utrecht als de twee andere UMC's, hebben in de enquête uitgebreider hun antwoorden toegelicht.

In de volgende paragrafen komen thema gewijs de resultaten aan bod. Deze thema's zijn geclusterd op de aard van de reacties die in de enquêtes naar voren kwamen.

7.2.1. Gebruik van het beoordelingsinstrument

Bijna alle respondenten vinden het duidelijk hoe het beoordelingsinstrument gebruikt dient te worden. Eén respondent geeft aan dat het wel omslachtig is. Een aantal adviezen die meegegeven zijn voor het gebruik van het instrument:

- Maak een apart kort stappenplan hoe het instrument gebruikt moet worden

- Maak het instrument zodanig dat er verplicht een toelichting moet worden ingevuld bij 'ja' en 'gedeeltelijk'

Daarnaast zijn er een aantal opmerkingen die verwijzen naar de wijze waarop het instrument geïmplementeerd zou kunnen worden.

- Verschillende respondenten, met name vanuit de ICT-organisatie, adviseren om deskundige begeleiding te bieden bij het invullen van het instrument. Er is specialistische kennis nodig om het instrument op de juiste wijze in te vullen. Ook zou een dergelijke aanpak helpen bij het verder expliciteren van antwoorden en een drempel vormen voor het 'sociaal wenselijk' antwoorden.
- Gezien de verscheidenheid aan vragen zijn deze niet allen door één functionaris te beantwoorden. De eerder genoemde begeleider, zou de vragen bij de verschillende deskundigen kunnen voorleggen.
- Als er een onafhankelijke begeleiding bij het invullen van het instrument aanwezig is, zou deze ook verder kunnen doorvragen naar 'bewijzen' bij de antwoorden. Als er bijvoorbeeld beantwoord wordt dat er een continuïteitsplan is, zou de begeleider ook kunnen vragen dit plan ook op te zoeken en te tonen. Het zijn adviezen van de UMC-functionarissen die te maken hebben met EDP-audits.

7.2.2. Eenduidigheid

De meeste geënquêteerden uiten de verwachting dat de vragenlijst op een eenduidige wijze ingevuld zal worden. Genoemd worden daarbij de specifieke en heldere vraagstelling. Een aantal kanttekeningen worden ook gemaakt:

- Nuance verschillen in antwoorden zijn mogelijk. Dit heeft te maken met onder andere kennis van de organisatie, bekendheid met de genoemde onderwerpen of de invalshoek van waaruit de vragenlijst wordt ingevuld
- Sommige vragen verdienen aanscherping, zodat de kans groter wordt dat deze eenduidig beantwoord worden. Vraag zoveel mogelijk naar concrete resultaten. Een vraag als 'Zijn risico's vastgesteld...?', kan nog sterker worden door te herformuleren naar "Zijn risico's schriftelijk vastgelegd...?" Dergelijke verbeteringen in formulering komen ook nog aan bod in paragraaf 7.2.4, waar deze per vraag zijn uitgewerkt.

7.2.3. Inzicht in continuïteitsbeheer

Een belangrijke doelstelling van het beoordelingsinstrument is om inzicht te krijgen in of het continuïteitsbeheer op alle aspecten goed is ingeregeld. Over het algemeen (15 van de 17 geënquêteerden) vinden de respondenten het beoordelingsinstrument een goed inzicht geven in de status van het continuïteitsbeheer. Verschillende keren wordt genoemd dat het overzicht 'mooi' of

'grafisch sterk' is. Niemand geeft aan dat het instrument onvoldoende inzicht geeft. Ook hier weer een aantal opmerkingen en suggesties.

- Er wordt door verschillende respondenten genoemd dat er te weinig inzicht is in hoe de berekening wordt gemaakt, hoe de weging tot stand is gekomen én wat de waarde van een bepaald percentage in de eindscore is. De suggestie wordt gedaan om samen met professionals nog eens kritisch naar de weging van de verschillende vragen te kijken.
- Een aantal respondenten merkt terecht op dat het beperkt aantal vragen bij de categorieën testen en onderhoud er voor zorgt dat antwoorden op deze vragen een onevenredig groot gewicht op de eindscore bepalen. De suggestie wordt gedaan om per categorie te streven naar een gelijk aantal vragen.
- Opgemerkt wordt dat de echte eindscores wellicht niet zo heel interessant zijn, maar wel een goede basis vormen voor discussie over de inrichting van het continuïteitsbeheer.

7.2.4. Inhoudelijke opmerkingen

Op de vraag of de vragen in het beoordelingsinstrument duidelijk zijn wordt uitgebreider antwoord gegeven. Van de 19 respondenten vermelden 12 respondenten dat de vragen duidelijk zijn. Bijna alle respondenten geven voorbeelden van onduidelijkheden en vragen die anders of beter geformuleerd kunnen worden. Niemand geeft aan dat de vragen in z'n algemeenheid onduidelijk zijn. In tabel 6 staan de inhoudelijke opmerkingen bij de vragen per vraag uitgewerkt. Algemene opmerkingen die hierbij nog gemaakt worden:

- Een viertal respondenten geeft aan dat op een aantal punten in de vragen wellicht teveel IT-jargon wordt gebruikt. Opvallend hierbij is dat het uitsluitend de mensen vanuit de ICT-organisatie zijn die deze opmerking plaatsen. Suggestie wordt gedaan om sommige begrippen verder toe te lichten
- Er wordt twee keer aangegeven dat het niet bij alle onderwerpen duidelijk is of de vragen nu om het specifieke proces gaat, ofwel om meer algemene procedures gaat. In het verlengde hiervan wordt de vraag gesteld of het beoordelingsinstrument ook gebruikt kan worden als het bedrijfsproces door meerdere systemen ondersteund wordt. Moet het beoordelingsinstrument dan meerdere keren worden ingevuld, of valt dit te combineren.

Aan de geënquêteerden is ook gevraagd of er vragen of aandachtsgebieden in het beoordelingsinstrument gemist worden. Iets meer dan de helft van de respondenten geeft aan het beoordelingsinstrument compleet te vinden. De andere respondenten doen suggesties voor aanvullingen:

- Leg bij de algemene gegevens ook vast hoe belangrijk het bedrijfsproces is. Wellicht zijn er verschillende categorieën te bedenken, waardoor ook het belang van goed continuïteitsbeheer op waarde kan worden geschat.

- Een vraag over externe communicatie wordt gemist. Bij calamiteiten is het ook van belang om helder te communiceren naar de 'buitenwereld'.
- Bij het onderwerp testen wordt de vraag naar een 'verantwoordelijke' voor het testproces gemist.
- Een suggestie wordt gedaan om meer aandacht te schenken aan interactie met de organisatie. Bijvoorbeeld afhankelijkheid van andere bedrijfsprocessen en aanwezigheid van voldoende gekwalificeerde gebruikers.
- Eén van de specialisten op het gebied van informatiebeveiliging mist in het instrument vragen over het crisisteam en crisisorganisatie, beheerder van het plan en voorlichting en training van medewerkers
- Dezelfde functionaris stelt ook voor het onderwerp 'testen' wat breder trekken. Onder testen kunnen ook andere controlevormen zoals verificatie, walkthrough en praktijktoets opgenomen worden.

Een meer fundamentele suggestie voor aanvulling van het instrument komt uit de hoek van mensen betrokken bij EDP-auditing. Het is bij auditing gebruikelijk te kijken naar zowel 'opzet', 'bestaan' en 'werking' van procedures. De eerste twee aspecten komen aan bod in het beoordelingsinstrument. Echter er zijn geen vragen naar 'werking'. Het gaat daarbij om het toetsen of de theorie ook in praktijk echt toegepast wordt. Bij een onderwerp als het maken van backups zou dan ook een vraag kunnen worden toegevoegd als "Is er in de laatste x maanden nog een backup teruggezet?" en "Deden zich bij het terugzetten van deze backup zich nog problemen voor?".

In onderstaande tabel staan de opmerkingen die specifiek op vragen van het beoordelingsinstrument betrekking hebben uitgewerkt.

Tabel 9 Enquête - Inhoudelijke opmerkingen per vraag

nr.	Vraagomschrijving	Reactie uit enquête
2. Organisatie		
2.4	Is het activeren van het continuïteitsplan beschreven als onderdeel van bestaande procedures rondom incident- en problemmanagement? (bijv. opgenomen als procedure bij de helpdesk)	<i>Wat wordt bedoeld met activeren van het continuïteitsplan</i>
2.6	Is vastgelegd welke acties onmiddellijk dienen te worden genomen bij incidenten met hoge impact (bijv. wanneer patiëntveiligheid in gevaar komt)?	<i>Is voor alle betrokkenen duidelijk wanneer patiëntveiligheid in gevaar is?</i> <i>Gaat het hier om afspraken over het bedrijfsproces of algemeen geldende afspraken?</i>
2.1 1	Is vastgelegd welke acties onmiddellijk dienen te worden genomen bij incidenten met hoge impact (bijv. wanneer patiëntveiligheid in gevaar komt)?	<i>Gaat het hier om afspraken over het bedrijfsproces of algemeen geldende afspraken?</i>
3. Risico- en Impactanalyse		
3.1	Zijn risico's vastgesteld, die onderbreking van het bedrijfsproces kunnen veroorzaken (bijvoorbeeld: storing van apparatuur, computervirus)	<i>Beter zou zijn "Zijn alle risico's vastgesteld..."</i>

3.2	Is vastgelegd welke systemen of applicaties het bedrijfsproces ondersteunen?	<i>Beter zou zijn "Is vastgelegd welke systemen of applicaties op welke manier het bedrijfsproces ondersteunen?"</i>
3.4	Is er een impactanalyse uitgevoerd om de gevolgen van de onderbrekingen vast te stellen (in de vorm van omvang van de schade en benodigde hersteltijd)	<i>Hoe voer je een impact analyse uit?</i>
3.5	Is vastgelegd waaruit de gevolgen van verstoring van het bedrijfsproces kunnen zijn (in termen van gevolgen voor patiënten, medewerkers, geïnvesteerde tijd, financiële gevolgen)?	<i>Zin is ongelukkig geformuleerd</i>
3.6	Is vastgesteld welke de maximale uitvalsduur van het bedrijfsproces is? (in termen van minuten, uren, dagen)	<i>Beter zou zijn "...maximaal toegestane uitvalsduur..."</i>
4. Maatregelen		
4.2	Zijn er fysieke maatregelen genomen ter voorkoming van uitval (bijv. afgesloten serverruimte)	<i>Vage formulering. Probeer specifieker te zijn zodat er eenduidiger beantwoord kan worden</i>

7.2.5. Vorm, layout

Hoewel niet specifiek in de enquête gevraagd, zijn in de reacties een aantal opmerkingen over de vorm van het beoordelingsinstrument gegeven. Soms in tegenspraak, waar het bijvoorbeeld gaat om de excelsheet met tabbladen per onderwerp. Waar de een dit handig en overzichtelijk vindt, ziet een ander er juist voordelen in om één lange lijst met vragen te presenteren. Suggesties die gedaan zijn:

- Laat het instrument omzetten naar een gebruikersvriendelijke webapplicatie.
- Het zou handig zijn om bij het overzicht op het laatste tabblad ook nog een rijtje met alle opmerkingen gepresenteerd te krijgen. Je ziet dan op één plek naast het totaaloverzicht van het diagram, ook nog de toelichting bij de antwoorden.
- Er zijn in het beoordelingsinstrument een aantal vragen die van elkaar afhankelijk zijn. Bijvoorbeeld als er geen continuïteitsplan is, is het antwoord op een aantal andere vragen ook per definitie 'nee'. Het instrument zou zo moeten werken dat die vragen dan overgeslagen kunnen worden.

7.2.6. Andere opmerkingen

De vorm van een enquête met open vragen, laat ook ruimte voor opmerkingen die niet direct het antwoord op vragen zijn.

Eén respondent mist nadrukkelijk aandacht voor continuïteitsbeheer buiten het domein van de informatievoorziening. Dit instrument zou te veel gericht zijn op continuïteit van informatievoorziening in plaats van continuïteit van het bedrijfsproces. "Dit is een valkuil voor ICT'ers". Zo wordt een maatregel als uitwijk van het hele bedrijfsproces genoemd. Op zich is de constatering terecht. Bij het opstellen van het instrument is echter een bewuste keuze gemaakt om de continuïteit van het bedrijfsproces in het kader van informatievoorziening te beschouwen en daarmee dus een bewust ingebouwde beperking.

Van de respondenten uit het UMC Utrecht geven er vijf ongevraagd aan graag te willen starten met het beoordelingsinstrument. Twee hiervan zijn werkzaam bij de Directie Informatie Technologie de anderen in een zorgdivisie.

Enkele respondenten doen de suggestie om het beoordelingsinstrument eens echt in te vullen voor een bedrijfsproces, om goed te kunnen beoordelen hoe dit uitpakt. Deze suggestie was al in het onderzoek verwerkt. In paragraaf 7.3 zal deze casestudy verder toegelicht worden.

7.3. Aanpak casestudy

Om de bruikbaarheid van het beoordelingsinstrument te toetsen is deze eenmalig voor een bestaand bedrijfsproces in het UMC Utrecht ingevuld. Hiervoor is het proces OK-planning genomen. Bij OK-planning gaat het om het plannen en toewijzen van resources, mensen en middelen en ruimte (operatiekamers). Met bijna 23.000 operatiezittingen per jaar [56] is een adequate ondersteuning van deze planning geen luxe, maar noodzaak.

Om een aantal redenen is juist voor dit proces gekozen in dit onderzoek. Het is een duidelijk voorbeeld van een bedrijfsproces welke afhankelijk is van geautomatiseerde informatievoorziening. Voor de OK-planning is vorig jaar een nieuw informatiesysteem geïmplementeerd. Hierdoor is het nog goed mogelijk om de afwegingen bij implementatie destijds rondom continuïteitsbeheer af te zetten tegenover de bevindingen nu. In het kader van dit onderzoek is bovendien een overzichtelijk proces gewenst. Het gaat bij OK-planning om een goed afgebakend proces.

Het beoordelingsinstrument is door de technisch projectleider, betrokken bij implementatie van het OK-planningssysteem, samen met de onderzoeker ingevuld. Deze projectleider is momenteel belast met technisch beheer van de applicatie. Vooraf is afgesproken dat de resultaten van het in gevulde beoordelingsinstrument níet integraal in het onderzoeksrapport gepubliceerd worden. Enerzijds omdat de beoordeling van dit specifieke bedrijfsproces geen deel uitmaakt van het beantwoorden van de onderzoeksvragen. Anderzijds zou de wetenschap dat de resultaten naar buiten zouden gaan de betrouwbaarheid van de score negatief kunnen beïnvloeden. Wél in dit rapport zijn de bevindingen ten aanzien van de bruikbaarheid van het instrument opgenomen.

In de vorm van een interview zijn een aantal vragen, opgenomen in bijlage 5, doorgenomen met de invuller van het beoordelingsinstrument. Dezelfde vragen zijn ook voorgelegd aan de security officer en het afdelingshoofd patiëntenzorg en koppelingen van de Directie Informatie Technologie. De laatste is tevens opdrachtgever van dit onderzoek.

7.3.1. Validiteit en betrouwbaarheid

Het mag duidelijk zijn dat deze enkele case alleen een eerste indruk kan geven van de praktische bruikbaarheid van het beoordelingsinstrument. Beperkingen van deze case zijn gelegen in:

- Het proces wordt voornamelijk ondersteund door één geautomatiseerd informatiesysteem
- Het beoordelingsinstrument is ingevuld door projectleider uit ICT-organisatie
- Slechts een beperkt aantal stakeholders hebben de resultaten uit het beoordelingsinstrument geëvalueerd.

Om beter de bruikbaarheid te kunnen toetsen zijn aanvullende casestudies aan te bevelen. Hierbij zouden complexere processen, zoals medische dossiervoering, waarbij veel meer informatiesystemen betrokken zijn kunnen worden beoordeeld. Bovendien zou het invullen van het beoordelingsinstrument ook door andere belanghebbenden, zoals de proceseigenaar kunnen worden uitgevoerd. Tenslotte zouden de diverse stakeholders, uit zowel ICT-organisatie als Business de resultaten dienen te waarderen.

7.4. Resultaten casestudy

De resultaten zijn in twee gedeelten te onderscheiden. Het invullen van het beoordelingsinstrument. Dit aspect kon alleen beoordeeld worden door de persoon die ook het instrument zelf ingevuld had. Het andere aspect betreft de bruikbaarheid van de resultaten van het beoordelingsinstrument. Hier hebben alle drie de belanghebbenden uitspraak over gedaan.

7.4.1. Invullen van het beoordelingsinstrument

Het invullen van het beoordelingsinstrument verloopt zonder problemen. Aangegeven wordt dat het wel handig is om het samen in te vullen met iemand die bekend is met de gebruikte concepten en terminologie. Zo wordt het concept 'continuïteitsplan' als zodanig wel herkend, echter niet duidelijk is of 'synoniemen' hiervoor ook beschouwd mogen worden als continuïteitsplan. Zo kan een 'handboek' beheer ook continuïteitsmaatregelen bevatten. Voor de invuller is het niet duidelijk of een dergelijk handboek daarmee ook als een continuïteitsplan behandeld kan worden.

Het invullen duurt niet langer dan een kwartier. Het wordt als prettig ervaren dat geen lange vragenlijst afgewerkt hoeft te worden. Bij het invullen van het beoordelingsinstrument wordt duidelijk dat verschillende vragen van elkaar 'afhankelijk' zijn. Als er geen continuïteitsplan is, kunnen veel andere vragen ook niet bevestigend worden ingevuld. Opgemerkt wordt dat sommige werkzaamheden in het technisch applicatiebeheer wel heel belangrijk zijn voor de continuïteit maar niet expliciet aan bod komen. Als voorbeeld wordt genoemd het testen van software voor implementatie.

7.4.2. Bruikbaarheid van resultaten beoordelingsinstrument

De invuller van het beoordelingsinstrument herkent de resultaten uit het beoordelingsinstrument. Het instrument maakt inzichtelijk dat rondom continuïteitsbeheer een aantal zaken niet formeel zijn vastgelegd. Het gaat daarbij met name om aspecten rondom onderhoud en testen. De inschatting van de invuller is dat dit op korte termijn nog weinig effect heeft. Echter naar verloop van tijd, als andere

mensen een rol krijgen in het proces is het risico reëel aanwezig dat het 'collectief geheugen' rondom het continuïteitsbeheer vervaagd.

Ook maakt het instrument duidelijk dat er weliswaar maatregelen op het gebied van continuïteitsbeheer zijn genomen, maar dat deze niet het gevolg zijn geweest van een risico- en impactanalyse. Hiermee is dus de kans aanwezig dat er weliswaar wel maatregelen, maar niet de juiste maatregelen ten behoeve van continuïteitsbeheer zijn genomen.

Op basis van het ingevulde instrument wordt duidelijk op welke aandachtsgebieden het proces verbeterd kan worden. De invuller, is als projectleider zelf nadrukkelijk betrokken geweest bij de implementatie van het OK-planningssysteem. Wanneer al tijdens dit project het beoordelingsinstrument was ingevuld, zou er direct duidelijkheid zijn geweest over de 'zwakke' plekken. In de huidige situatie is dit een bij een 'gevoel' gebleven en heeft daarmee ook niet tot discussie geleid. Er hebben zich echter in praktijk tot nog toe geen incidenten voorgedaan waarvan aangenomen kan worden dat een ander ingeregeld continuïteitsbeheer hier consequenties op zouden hebben gehad.

De twee andere personen aan wie het resultaat is voorgelegd zijn unaniem in hun oordeel. Het ingevulde instrument geeft een reëel beeld van de status van het continuïteitsbeheer. Het beeld bevestigt het gevoel wat er al was over de goede en mindere aspecten, maar het wordt als belangrijk ervaren dat dit ook 'zwart op wit' staat. Beide zijn ook van mening dat, wanneer het instrument bij implementatie van het OK-systeem was ingevoerd, er andere maatregelen zouden zijn genomen. De inschatting is overigens niet dat deze andere maatregelen eventuele problemen of storingen in het systeem zouden hebben voorkomen. Tot slot wordt door zowel opdrachtgever als security officer benadrukt dat een ingevuld beoordelingsinstrument in ieder geval voor alle betrokkenen heel transparant en inzichtelijk maakt voor welke keuzes de organisatie staat. Ook dan kan wel overwogen ervoor gekozen worden bepaalde maatregelen rondom continuïteitsbeheer níet te nemen. Dit is dan wel een bewust genomen keuze.

Geconcludeerd wordt dat het beoordelingsinstrument in de huidige vorm een aanvullende waarde heeft bij de bewustwording rondom continuïteitsbeheer.

7.5. *Samenvatting*

Het nieuwe beoordelingsinstrument is op twee manieren gevalideerd. Middels een enquête is bij verschillende belanghebbenden het oordeel over verschillende aspecten van het beoordelingsinstrument gevraagd. Ook is in een casestudy het beoordelingsinstrument in praktijk getoetst.

De enquête leverde een schat aan zinvolle respons op. In z'n algemeenheid kan gesteld worden dat de respondent het beoordelingsinstrument in gebruik duidelijk vinden. Ook geeft het instrument

voldoende inzicht in de status van het continuïteitsbeheer en is er een redelijke mate van eenduidigheid te verwachten. Er worden verschillende suggesties en opmerkingen geplaatst. Zo is meer aandacht nodig voor het tot stand komen van de uiteindelijke score. Ook is onvoldoende inzichtelijk hoe de berekening van de scores verloopt. Aandacht wordt bovendien gevraagd voor een kritische blik op de weging van de verschillende vragen. Nog duidelijker mag het instrument tonen wat streefwaarden voor de verschillende aspecten zijn, eventueel ondersteund met kleurcoderingen. Geadviseerd wordt om het invullen van het instrument samen te doen met iemand die deskundig is op het gebied van continuïteitsbeheer en bij voorkeur geen direct belang heeft bij de uitslag.

De casestudy bevestigt een aantal van de bevindingen van de enquête. Het beoordelingsinstrument wijst zichzelf, maar voor het goed interpreteren van de vragen is hulp van een 'deskundige' wel gewenst. De ondervraagden zijn unaniem in hun oordeel dat het instrument goed zicht geeft op de stand van continuïteitsbeheer. Het gebruik van het beoordelingsinstrument zou ook daadwerkelijk invloed hebben gehad op de genomen maatregelen bij de ingebruikname van een nieuw informatiesysteem.

8. Conclusies en verder onderzoek

Het onderwerp Business Continuity Management staat in toenemende belangstelling. Dit geldt in het bijzonder voor de gezondheidszorg waar de afhankelijkheid van zorgkritische ICT snel toeneemt. De centrale vraag in dit onderzoek is hoe bepaald kan worden of er voldoende gedaan wordt om de continuïteit van de processen, die ondersteund worden door ICT, te waarborgen. In dit hoofdstuk zal een antwoord gegeven worden op de onderzoeksvragen. Ook volgen aanbevelingen voor verder onderzoek.

8.1. *Antwoord op de onderzoeksvragen*

In hoofdstuk 1 is de hoofdvraag van dit onderzoek gepresenteerd:

“Hoe kan een ziekenhuis bij implementatieprojecten van zorgkritische ICT beoordelen of voldoende maatregelen zijn genomen voor het vaststellen en verminderen van risico's, beperken van gevolgen van incidenten en tijdig hervatten van werkzaamheden in het geval van uitval van deze systemen?”

Om deze onderzoeksvraag te kunnen beantwoorden zijn een aantal deelvragen geformuleerd. Deze zullen achtereenvolgens beantwoord worden, om hierna het antwoord op de hoofdvraag te kunnen formuleren.

- 1) *Welke aspecten zijn van belang in BCM rondom ICT, essentieel voor uitvoering van directe patiëntenzorg?*

Het proces continuïteitsbeheer kent de fasen analyse, maatregelen, evaluatie, testen en onderhoud. Er is nationaal en internationaal steeds meer regelgeving en standaarden op het gebied van informatiebeveiliging in het algemeen en continuïteitsbeheer in het bijzonder. Voor de Nederlandse gezondheidszorg is NEN 7510 hierbij belangrijk. Continuïteitsbeheer in de gezondheidszorg kan letterlijk om 'leven en dood' gaan, hetgeen het belang hiervan nog eens extra onderstreept.

- 2) *Welke instrumenten zijn beschikbaar voor het beoordelen van BCM?*

Er zijn verschillende instrumenten voor het beoordelen van BCM. Het gaat hier om vragenlijsten, checklists of audit-tools. Sommigen zijn gekoppeld aan een maturity-model, welke de mate van volwassenheid van de organisatie inzichtelijk moet maken. Een vijftal instrumenten, besproken in hoofdstuk 3 zijn in dit onderzoek nader bestudeerd.

- 3) *Aan welke criteria dient een beoordelingsinstrument voor BCM te voldoen?*

Uit de literatuur zijn criteria gevonden voor een beoordelingsinstrument voor BCM. Deze zijn in dit onderzoek voorgelegd aan stakeholders in het UMC Utrecht. Dit heeft geresulteerd in een matrix met criteria die zijn te onderscheiden in 'inhoudelijke aspecten', 'kwaliteitsaspecten' en aspecten die te maken hebben met de 'scope' van de toepassing van het beoordelingsinstrument. In hoofdstuk 4 zijn deze definitieve criteria uiteengezet.

- 4) *Welke van de gevonden beoordelingsinstrumenten is het meest geschikt als referentie instrument?*

Van de beoordeelde instrumenten is de checklist, behorende bij de Code voor Informatiebeveiliging [42] de enige die, op basis van de gedefinieerde criteria, als goed beoordeeld wordt. De andere getoetste instrumenten kennen echter ook hun kwaliteiten, bijvoorbeeld met betrekking tot de presentatie van de resultaten.

- 5) *Zijn er aanpassingen nodig in het referentie instrument om te voldoen aan de gestelde criteria?*

De verschillende instrumenten hebben eigen sterke punten en zijn hierin complementair aan elkaar. Om de kwaliteiten van de verschillende instrumenten ten volle kunnen benutten is gekozen voor de ontwikkeling van een nieuw beoordelingsinstrument welke de beste eigenschappen combineert.

- 6) *Welke aanpassingen zijn nodig om het referentie instrument te laten voldoen aan de gestelde criteria?*

Op basis van de beste onderdelen van de verschillende beoordelingsinstrumenten is een nieuw beoordelingsinstrument ontwikkeld. De implementatie van dit instrument is gedaan in de vorm van een Excel werkmap. Schermafdrukken hiervan zijn opgenomen in bijlage 3.

Dit brengt ons terug bij de hoofdvraag:

“Hoe kan een ziekenhuis bij implementatieprojecten van zorgkritische ICT beoordelen of voldoende maatregelen zijn genomen voor het vaststellen en verminderen van risico's, beperken van gevolgen van incidenten en tijdig hervatten van werkzaamheden in het geval van uitval van deze systemen?”

Het ontwikkelde beoordelingsinstrument lijkt een goed hulpmiddel bij het beoordelen van de status van het continuïteitsbeheer. Dit wordt bevestigd in de enquêtes waarin het instrument aan verschillende belanghebbenden wordt voorgelegd. Ook uit de casestudy blijkt dat het

beoordelingsinstrument inzicht geeft in de goede en mindere kanten van het continuïteitsbeheer bij het betreffende proces. Er zijn in dit onderzoek door de betrokkenen ook verschillende suggesties gedaan om het instrument nog verder te kunnen verbeteren. Geheel in de lijn van het cyclische proces van continuïteitsbeheer zal het nieuwe beoordelingsinstrument ook verder verbeterd moeten worden. Deze verbetering valt echter buiten de scope van dit onderzoek. Met het oog op de praktische inzet van dit instrument in het UMC Utrecht zal in de komende tijd, op basis van de suggesties, nog verdere aanpassing van het instrument plaatsvinden.

8.2. *Vervolgstappen en aanbevelingen*

Met het nieuwe beoordelingsinstrument als ‘vastbaar’ resultaat van dit onderzoek, resten er nog verschillende vragen.

Een belangrijke vraag bij het gebruik van een dergelijk beoordelingsinstrument is hoe dit in praktijk te implementeren. In dit onderzoek zijn, onder andere vanuit de interviews en enquêtes, al enige aanbevelingen gedaan. Zo zou implementatie van een nieuw informatiesysteem een goed moment kunnen zijn om een meting te doen. Maar ook de vraag wie het instrument zou moeten invullen, bijvoorbeeld de proceseigenaar of een ‘onafhankelijke auditor’, zijn vragen die in dit onderzoek niet direct beantwoord zijn. Het zijn vragen waar de organisatie, die dit instrument gaat gebruiken, een antwoord op moet vinden.

In het onderzoek zijn verschillende suggesties verzameld voor verdere verbetering van het instrument. Deze hebben bijvoorbeeld te maken met de presentatievorm, waarbij suggesties worden gedaan voor een gebruikersvriendelijkere en ‘intelligentere’ applicatie. Maar ook de weging die aan de verschillende vragen in het beoordelingsinstrument kan worden gegeven, vraagt nog een nadere analyse. Een en ander kan beter in kaart worden gebracht door het instrument enige tijd in praktijk te gebruiken en daarna de bruikbaarheid nogmaals te valideren.

Dit onderzoek heeft zich vrij snel gericht op het beoordelingsinstrument van BCM. Echter het gebruik van het beoordelingsinstrument mag geen doel op zich zijn. De organisatie die dit instrument gaat gebruiken zal een bredere visie en beleid op het gebied van BCM moeten ontwikkelen, waar dit instrument een plaats in kan hebben.

Een goed ingericht continuïteitsbeheer in de gezondheidszorg vertegenwoordigt een belangrijke waarde. Al eerder werd benadrukt dat het een kwestie van ‘leven en dood’ kan zijn. Maar goed continuïteitsbeheer en uitgebreide maatregelen voor disaster recovery kent ook een hoge prijs. Een goed onderwerp voor verder onderzoek zou kunnen zijn om deze waarde van continuïteit echt te kwantificeren. Dat kan helpen om verantwoorde afwegingen te maken bij het inrichten van continuïteitsbeheer en bijbehorende kosten.

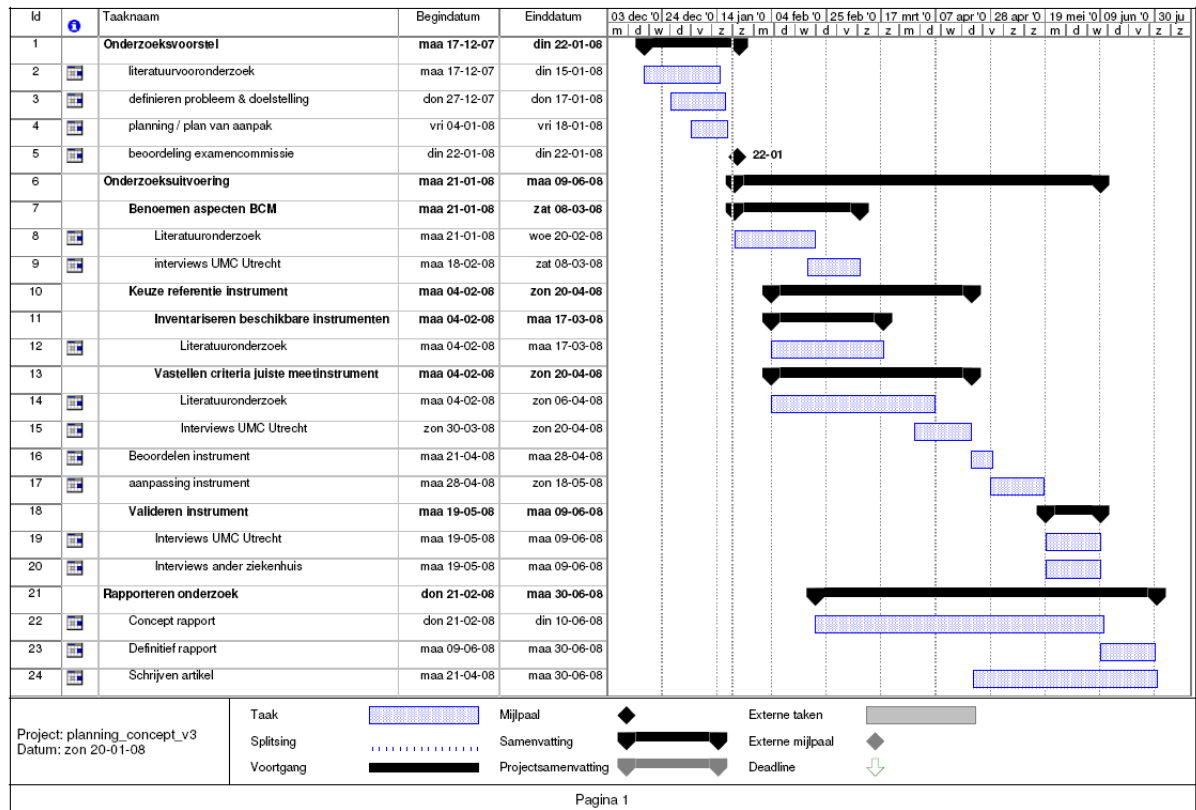
9. Bronnen

1. NICTIZ. *Over ICT in de zorg*. 2007 [cited 2008 13-01-2008]; Available from: <http://www.nictiz.nl/?mid=101&pg=134>.
2. van Ginneken, A.M., *The computerized patient record: balancing effort and benefit*. International journal of medical informatics, 2002. **65**(2): p. 97 - 119.
3. IGZ, *ICT in ziekenhuizen. Beveiliging van informatie nog onvoldoende voor een papierloze patiëntenzorg*. 2004, Inspectie voor de Gezondheidszorg: Den Haag. p. 28.
4. HIMMS, *19th Annual 2008 HIMSS Leadership Survey*. 2008, HIMMS (Healthcare Information and Management Systems Society).
5. NEN, *Nederlandse norm NEN 7510 (nl) Medische informatica - Informatiebeveiliging in de zorg - Algemeen*, NEN, Editor. 2004: Delft. p. 39.
6. Leegwater, D., *Business Continuity Management in de zorg: een gezamenlijke operatie*. ZORGSpecial, Maandblad voor Bestuur, Directies en hoger Management in de zorgsector, 2005. **6**: p. 4-8.
7. DIT, *Grensverleggend samenwerken. ICT-Beleidsplan UMC Utrecht 2006-2010*. 2005, UMC Utrecht: Utrecht. p. 28.
8. Baarda, D.B., M.P.M.d. Goede, and V.d. Meer-Middelburg, *Basisboek Interviewen*. 2007, Groningen: Wolters-Noordhoff. 128.
9. Saunders, M., P. Lewis, and A. Thornhill, *Research methods for business students*. 3rd ed. ed. 2003, Harlow ; New York: Prentice Hall. xviii, 504 p.
10. *Over UMC Utrecht*. 2006 [cited 2008 2008-05-01]; Available from: <http://www.umcutrecht.nl/overumcutrecht/>.
11. drj.com. *Business Continuity Glossary*. [cited 2008 february 26]; Available from: <http://www.drj.com/glossary/drjglossary.html>.
12. BCPWHO. *Business Continuity Management. Definitions*. 2007 [cited; Available from: <http://www.bcpwho.org/200what/200a.htm>].
13. BCI, *Business Continuity Management Good Practice Guidelines 2008*. 2007, Business Continuity Institute. p. 6.
14. Bron, J.v., G. Kemmerling, and D. Pondman, *IT Service Management, een introductie*. V4.0 ed. 2004: Van Haren Publishing. 264.
15. Smit, N., *Business Continuity Management. A maturity model*, in *Informatics & Economics*. 2005, Erasmus University Rotterdam: Rotterdam. p. 130.
16. NEN, *Nederlandse norm NEN 7511-1 (nl) Medische informatica - Informatiebeveiliging in de zorg - Toetsbaar voorschrift bij NEN 7510 voor complexe organisaties*, NEN, Editor. 2005: Delft. p. 34-35.
17. Gotaishi, M., *Business Continuity Planning beyond ISO17799*, in *GIAC Security Essentials. Practical Assignment version 1.4. Option 1*. 2004, SANS Institute. p. 3.

18. itsmf. *Continuity Management*. 2008 [cited 2008 february 1]; Available from: http://www.itsmf.nl/index.php?option=com_content&task=view&id=41&Itemid=7.
19. ITGI, *COBIT 4.1 Executive Summary*. 2007, IT Governance Institute: Rolling Meadows. p. 29.
20. Deming, W.E., *Out of the crisis : quality, productivity and competitive position*. 1986, Cambridge: Cambridge University Press. xiii,507p.
21. BCI, *Business Continuity Management Good Practice Guidelines 2008*. 2007, Business Continuity Institute. p. 7.
22. Barnes, J.C., *A guide to business continuity planning*. 2001, Chichester: Wiley. viii, 184 p.
23. Helms, R.W., et al., *An integral IT continuity framework for undisrupted business operations*, in *Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06) - Volume 00*. 2006, IEEE Computer Society.
24. Cazemier, J. and D. Leegwater, *Business Continuity Management. BCM-standaard helpt niet tijdens de crisis*. IT SERVICE MAGAZINE, 2007. 4: p. 12-15.
25. NEN, *Handboek NEN7510*, NEN, Editor. 2005, NEN.
26. BCI, *Business Continuity Management Good Practice Guidelines 2008*. 2007, Business Continuity Institute. p. 16.
27. Honour, D. *Business continuity standards*. 2007 [cited 2008 31-5-2008]; Available from: <http://www.continuitycentral.com/feature0496.htm>.
28. Coleman, P. *Business Continuity Planning in the healthcare environment* [cited 2008 16-01-2008]; Available from: http://www.disaster-resource.com/articles/bus_cont_healthcare_unabridged_coleman.shtml.
29. NEN. *Over NEN7510*. 2006 [cited 2008 february 1]; Available from: www.nen7510.org.
30. Erk, R.A.v. and J.G.v. Dongen, *Adviesrapport ICT-beveiliging in de Zorg*. 2006, Interpay - Ministerie van VWS. p. 19.
31. Campbell, E.M., et al., *Types of Unintended Consequences Related to Computerized Provider Order Entry*, American Medical Informatics Association.
32. Ash, J.S., et al., *The Extent and Importance of Unintended Consequences Related to Computerized Provider Order Entry*. Journal of the American Medical Informatics Association, 2007. 14(4): p. 415-423.
33. Roman, M., *Life or Death: Business Continuity in Healthcare*. For the Record, 2006. 18(4).
34. NEN, *1312-1 Continuïteitsstrategie*, in *Handboek NEN7510*, NEN, Editor. 2005, NEN.
35. Frigg, R. and S. Hartmann. *Models in Science*. Stanford Encyclopedia of Philosophy 2006 27 february 2006 [cited 2008 2008-07-01]; Available from: <http://plato.stanford.edu/entries/models-science/>.
36. CarnegieMellon, *Capability Maturity Model (R) Integration (CMMI(R)) Version 1.2 Overview*, C.M. University, Editor. 2007, Carnegie Mellon University.
37. Paulk, M.C., *A History of the Capability Maturity Model for Software*. 2001, Software Engineering Institute, Carnegie Mellon University: Pittsburgh.

38. Schoemaker, J.W.R., *Contuïteitsstrategie Erasmus MC "hoe waarborgen wij de continuïteit van de vitale bedrijfsprocessen in geval van een calamiteit?"* 2005, Erasmus MC: Rotterdam. p. 9-10.
39. Peterson, D., *Vendor Resiliency Business Continuity Planning Questionnaire*. 2003, Merrill Lynch. p. 5.
40. Qubus, *Monitor Informatiebeveiliging 2.008*, in *Vragenlijst Informatiebeveiliging in de zorg*, KPMG Qubus Competence Center. p. 35-37.
41. Oud, E.J., *Praktijkgids Code voor informatiebeveiliging*. 2002, Academic Service. p. 54-60.
42. Kennisnet. *Links rond ict en veiligheid* [cited 2008 June 14, 2008]; Available from: <http://www.ictopschool.net/software/veiligheid/Checklist-D1-implementatie-Code-voor-Informatiebeveiliging.pdf>.
43. Smith, D.J., *BSI PAS56 Evaluation Criteria Workbook*. 2002, The Business Continuity Institute.
44. NHS. *Knowledge Base. NHS Connecting for health*. [cited 2008 June 14, 2008]; Available from: [https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseNew/Audit%20Programme%20-%20Business%20Continuity%20\(Detailed\).xls](https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseNew/Audit%20Programme%20-%20Business%20Continuity%20(Detailed).xls).
45. [cited 2008 June 14, 2008]; Available from: www.rudnicki.com.pl/pub/BCI_PAS-56.xls.
46. Bakker, T., *BCM (PAS56) en CobIT*. Informatiebeveiliging, 2006. **314**: p. 33-37.
47. VirtualCorporation, *Business Continuity Maturity Model*. 2007, Virtual Corporation Inc.: Budd Lake.
48. VirtualCorporation. *BCMM Survey*. 2002 [cited 2008 2008-03-01]; Available from: http://virtual-corp.net/survey/bcm_survey.html.
49. Zee, F.v.d., *Kennisverwerving in de Empirische Wetenschappen*. 2004, Groningen: BMOOO.
50. Cooper, D., *Improving safety culture : a practical guide*. 1998, Chichester: Wiley. xv, 302p.
51. Speelman, D. *Inleiding praktische statistiek voor linguïstische toepassingen*. 1998 [cited 2008 06]; 01]. Available from: <http://www.ling.arts.kuleuven.ac.be/genling/statistiek/>.
52. Thurstone, L.L., *Attitudes Can Be Measured*. American Journal of Sociology, 1928. **33**(4): p. 529.
53. Pelsmacker, P.D. and P.V. Kenhove, *Marktonderzoek: methoden en toepassingen*. 2006: Pearson Education. 515.
54. Apel, L. *RADAR CHART/SPIDER CHART*. 1996 [cited; Available from: <http://web2.concordia.ca/Quality/tools/23radar.pdf>.
55. Trochim, W.M.K. *The Research Methods Knowledge Base*. [Internet WWW page] 2006 October 20, 2006 [cited 2008 2008-07-01]; 2nd:[Available from: <http://www.socialresearchmethods.net/kb/>.
56. *Jaarverslag 2006*. Divisie Perioperatieve zorg en spoedeisende hulp 2007 [cited 2008 June 10, 2008]; Available from: <http://www.umcutrecht.nl/jaarverslag2006/0311.htm>.

Bijlage 1: Planning onderzoek



Figuur 14 Planning Onderzoek Gannt Chart

Bijlage 2: Interview Toetsing aspecten BCM en criteria Meetinstrument

Introductie

Bedankt voor de gelegenheid dit interview te houden. **Anonimiteit:** Bij de verwerking van de gegevens zal ik er voor zorgen dat antwoorden niet herleidbaar zijn naar u als persoon. Ik zou graag dit interview willen **opnemen**, zodat ik het thuis verder kan uitwerken, heeft u hier bezwaar tegen.

- Onderwerp van Thesis is continuïteitsbeheer voor zorgkritische ICT-systemen. Bij continuïteitsbeheer, ook wel BCM, gaat het om het zorgen voor **continuïteit van bedrijfsprocessen**. Het gaat dan om **identificeren van bedreigingen** (bijv. stroomuitval), **preventieve maatregelen** (noodstroom voorziening) en **correctieve maatregelen** (noodprocedures, uitwijkprocedures). In mijn onderzoek kijk ik welk meetinstrument het beste geschikt is om te meten welke maatregelen zijn genomen, en waar zaken ontbreken. Denk bij een meetinstrument aan een checklist of een vragenlijst.

Bij **invoeringstrajecten van nieuwe ICT-ondersteuning** in de zorg kan dan standaard een check worden uitgevoerd die laat zien hoe het gesteld is met het continuïteitsbeheer. Ik onderzoek **welke meetinstrumenten er zijn**, of deze geschikt zijn of evt. aanpassing nodig zijn. Belangrijk is om te bepalen aan welke eisen dit moet voldoen.

Doel van het interview

- Algemene vragen, om inzicht te krijgen in positie tov BCM
- De criteria voor een meetinstrument toetsen en wegen.
- Bepalen welke personen / functionarissen hierover zeker mee moeten denken

Is bovenstaande duidelijk, zijn hier nog vragen over?

Allereerst start ik met wat algemene vragen rondom BCM

- 1) Had u al eerder gehoord van continuïteitsbeheer of BCM? Heeft u in u werk hier al eerder mee te maken gehad? Kunt u dit toelichten?
- 2) Heeft u zelf een rol of verantwoordelijkheid in het continuïteitsbeheer. Zo ja, kunt u deze verder toelichten aan de hand van een voorbeeld
- 3) Wie is of zijn naar uw mening verantwoordelijk voor het proces van continuïteitsbeheer?

Criteria meetinstrument

Een goed meetinstrument voor het meten van maatregelen op het gebied van continuïteitsbeheer zal aan een aantal eisen moeten voldoen. Onderstaand zijn een aantal van deze eisen gesteld. Die zal ik eerst doornemen. Ik begin met het opsommen van inhoudelijke aspecten waaraan het meetinstrument zou moeten voldoen. Vervolgens noem ik ook aspecten die meer over de kwaliteit van het meetinstrument zeggen.

Inhoudelijke aspecten		
Risicoanalyse		
Vaststellen bedreigingen	Het benoemen van mogelijke bedreigende incidenten voor continuïteit van het betreffende bedrijfsproces	[22], [16]
Vaststellen waarschijnlijkheid	Het benoemen van de waarschijnlijkheid dat het bedreigende incident plaatsvindt	[23]
Business Impact Analyse		
Vaststellen impact	Identificeren, kwantificeren en kwalificeren van schade ontstaan door verstoring van bedrijfsproces	[13], [22]
Vaststellen MUD	Vaststellen maximale duur van verstoring proces	[16]
Vaststellen MGv	Vaststellen maximaal toelaatbaar verlies aan gegevens	[16]
Maatregelen		
Vaststellen preventieve maatregelen	Maatregelen ter voorkoming van verstoring of afwending dreiging van incident	[6]
Vaststellen correctieve maatregelen	Maatregelen om in het geval van een incident zo snel mogelijk bedrijfsproces te kunnen hervatten en evt. schade te herstellen	[6]
Evaluatie		
Testen maatregelen	Het periodiek testen van maatregelen	[22]
Onderhoud maatregelen	Bijstellen van maatregelen ingebed in reguliere wijzigingsbeheerprocessen	[22]

Criterion	Omschrijving	Bron
kwaliteitsaspecten		
Efficiëntie	De juiste vragen worden gesteld, zodat meting efficiënt plaatsvindt.	[49]
Objectief	Onderzoeker mag geen invloed hebben op het resultaat. Meting uitgevoerd door verschillende personen moet zelfde uitslag geven.	[49]
Normerend	het meetinstrument moet voldoende discriminerend vermogen hebben. Het moet een meetlat zijn waardoor vergelijking tussen verschillende metingen mogelijk worden	[49]
Valide	De resultaten van de test zeggen daadwerkelijk iets over het gemeten onderwerp (ic continuïteitsbeheer)	[49]
Voldoen aan regelgeving	Wordt in het meetinstrument getoetst op de aspecten zoals die in de NEN-norm voor	[29]

	informatiebeveiliging (NEN7510) voor continuïteitsbeheer zijn vastgesteld. Deze norm is straks leidend bij het landelijk EPD.	
Scope van meetinstrument		
<i>Metten op niveau bedrijfsproces (detailniveau)</i>	De scope van de meting is het bedrijfsproces (een BCM meting kan bijv. ook op het niveau van de organisatie als geheel plaatsvinden)	[25]
<i>Metten op proces patiëntenzorg (domein)</i>	De scope van de meting is op het domein patiëntenzorg.	[33]
<i>Metten op informatievoorziening</i>	De scope van de meting beperkt zich tot continuïteit van de informatievoorziening	
<i>Zinvol resultaat na één meting</i>	Het meetinstrument wordt ingezet bij evalueren van projecten en zal dan ook in een eenmalige meting moeten kunnen voldoen.	

Is duidelijk wat hiermee bedoeld wordt?

In de volgende tabel staan alle criteria op een rijtje.

4) Met betrekking tot de 'inhoudelijke aspecten', mist u hier nog zaken, opmerkingen suggesties, aanvullingen?

1) Geef aan hoe belangrijk u de afzonderlijke criteria beoordeeld.

2) Geef een volgorde van belangrijkheid aan 1= belangrijkst, 7 minst belangrijk

6) Zijn er eisen die u mist in deze opsomming. Waar zou een goed meetinstrument aan moeten voldoen

7) Kent u instrumenten die continuïteitsbeheer meten? Zo ja welke?

8) Is één van de instrumenten die u kent geschikt voor gebruik in het UMC Utrecht? Zo ja welke + toelichting? Zo nee, waarom niet?

Stakeholders

- 9) Bij het proces van continuïteitsbeheer zijn verschillende belanghebbenden. Welke functionarissen zijn belangrijk bij het beoordelen van een meetinstrument? (Denk in termen van functies, arts, manager bedrijfsvoering etc.)

- 10) Heeft u verder nog opmerkingen of aanvullingen?

Hartelijk dank voor de medewerking. Ik zal het onderzoeksresultaat terugkoppelen

Aan welke criteria dient een meetinstrument voor het meten van continuïteitsbeheer te voldoen?

Inhoudelijke aspecten meetinstrument

Inhoudelijke aspecten
Risicoanalyse
Vaststellen bedreigingen
Vaststellen waarschijnlijkheid
Business Impact Analyse
Vaststellen impact
Vaststellen MUD
Vaststellen MGv
Maatregelen
Vaststellen preventieve maatregelen
Vaststellen correctieve maatregelen
Evaluatie
Testen maatregelen
Onderhoud maatregelen

Kwaliteitseisen aan meetinstrument	Ze er Onbelangrijk	Onbelangrijk	Neutraal	Belangrijk	Ze er Belangrijk	Volgorde van belang (1= meest belangrijk, 5=minst van belang)
- Efficiënt in te vullen						
- Objectief						
- Normerend						
- Valide						
- Voldoet aan regelgeving						
Scoping meetinstrument	Ze er Onbelangrijk	Onbelangrijk	Neutraal	Belangrijk	Ze er Belangrijk	Volgorde van Belang (1=meest belangrijk, 4= minst van belang)
- Meet op niveau van bedrijfsproces						
- Gericht op patiëntenzorg						
- Gericht op informatievoorziening						
- Zinvol resultaat na één meting						

Bijlage 3: Schermafdrucken nieuw beoordelingsinstrument

Microsoft Excel - BeoordelingsInstrument_continuïteitsbeheer_0.2_ingevuld.xls

Bestand Bewerken Beeld Invoegen Opmaak Extra Data Venster Help Typ een vraag voor hulp

I23

1 A B C D E F G H I J K L M

2 **Beoordelingsinstrument continuïteitsbeheer informatievoorziening**

3 versie 0.2

4  

5 **Algemene gegevens**

6 **Risicoanalyse**

7 1.0	Naam bedrijfsproces	Poliklinisch afspraken maken
8 1.1	Datum beoordeling	05-05-2008
9 1.2	Beoordeling door (naam)	Peter Janssen
10 1.3	Beoordeling door (functie)	projectmedewerker nieuw afsprakensysteem
11 1.4	Naam proceseigenaar	Riet de Graaf
12 1.5	Functie proceseigenaar	Manager zorg divisie Chirurgie

13 **Toelichting bij beoordelingsinstrument**

14

15 **Wat is het beoordelingsinstrument continuïteitsbeheer informatievoorziening?**

16 Dit beoordelingsinstrument kan gebruikt worden om inzicht te krijgen in de status van het continuïteitsbeheer voor een bedrijfsproces. De resultaten zijn

17 slechts indicatief.

18

19 **BELANGRIJK:** Iedere organisatie zal zelf dienen te bepalen hoe het beste voldaan kan worden aan eigen richtlijnen, normen, wet- en regelgeving op het

20 gebied van continuïteitsbeheer.

21

22 **Hoe dit beoordelingsinstrument te gebruiken?**

23 Werk de tabbladen door en beantwoord alle vragen. Als antwoordmogelijkheden kunnen uitsluitend 'Ja', 'Nee', 'Gedeeltelijk', 'Onbekend' worden gebruikt.

24 Achter ieder antwoord is ruimte voor toelichting of evt. suggesties ter verbetering.

25

26 Op tabblad '7. Overzicht', is in de vorm van een radardiagram zichtbaar hoe op de verschillende aspecten gemiddeld gescoord is.

27

28 **Hoe is dit beoordelingsinstrument tot stand gekomen?**

29 Dit instrument is gemaakt door Peter Vermeulen als onderdeel van een thesis voor de studie Master of Informatics aan Hogeschool Utrecht. Dit

30 beoordelingsinstrument is nieuw ontwikkeld, inspiratie is opgedaan vanuit bestaande instrumenten:

31 - checklist code voor informatiebeveiliging

32 - checklist continuïteitsplanning NEN7510

33 - audit workflow BASE6

34

35 **1. Algemene gegevens** / 2. Organisatie / 3. Risico- en Impactanalyse / 4. Maatregelen / 5. Testen / 6. Onderhoud / 7. Overzicht /

Gereed NUM

De ingevulde gegevens dienen slechts als voorbeeld en zijn geen beschrijving van de werkelijke situatie

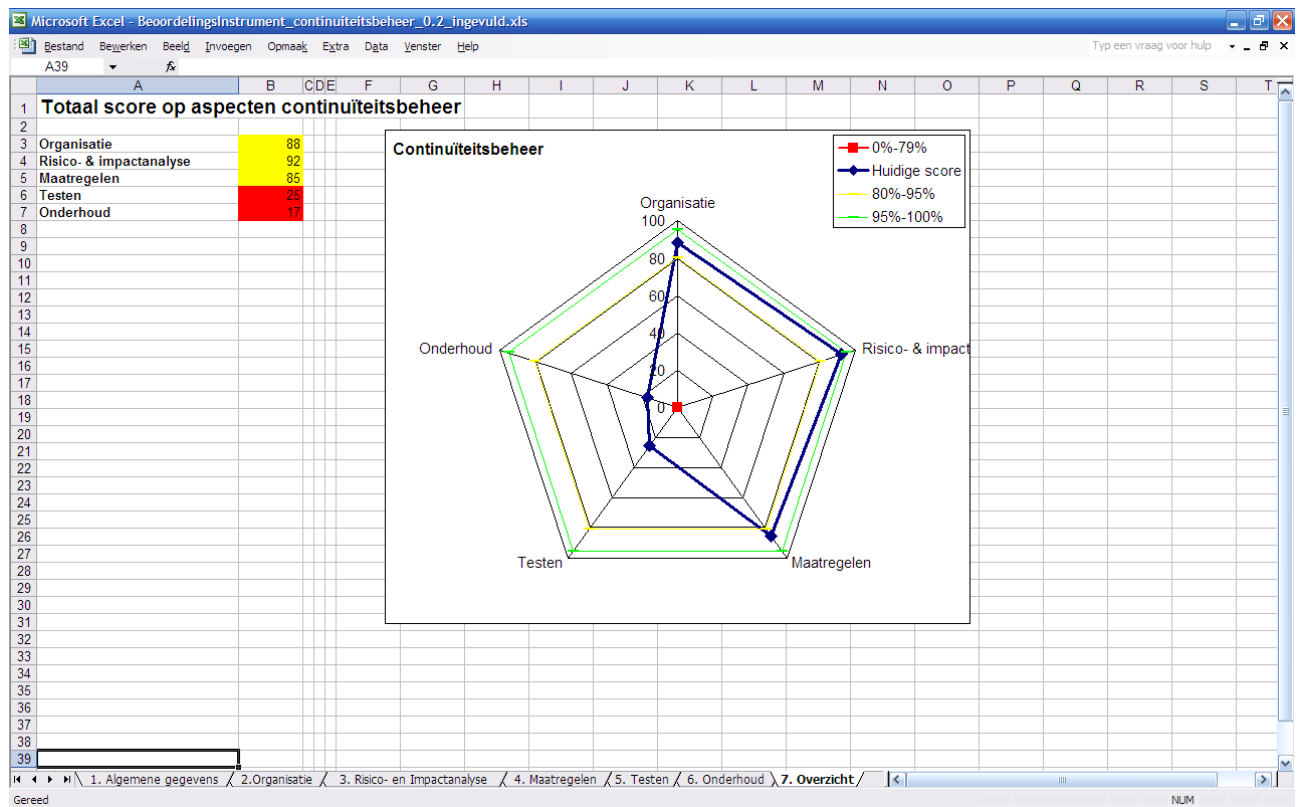
Microsoft Excel - BeoordelingsInstrument_continuïteitsbeheer_0.2_ingevuld.xls						
Bestand Beveiligen Invoegen Opmaak Extra Data Venster Help						
C3 Ja						
Typ een vraag voor hulp						
A	B	C	D	E	F	G
Vraagnr	Vraag	Antwoord	Opmerkingen / Voorstel ter verbetering	Score	Gewicht	Gewogen score
1	Organisatie continuïteitsbeheer					
2	2.1 Is er een continuïteitsplan?	Ja		100	1	100
4	2.2 Is het continuïteitsplan aan een eigenaar toegewezen?	Ja		100	1	100
5	2.3 Is het continuïteitsplan goedgekeurd door management van betrokken Divisie/Directie en centrale ICT?	Ja		100	1	100
6	2.4 Is het activeren van het continuïteitsplan beschreven als onderdeel van bestaande procedures rondom incident- en probleemmanagement? (bijv. opgenomen als procedure bij de helpdesk)	Gedeeltelijk	Is wel de afspraak, maar moet nog opgenomen worden in draaiboek	50	1	50
7	2.5 Zijn de condities vastgelegd om het continuïteitsplan te activeren? (zoals hoe de situatie beoordeeld moet worden, wie daarbij betrokken moet zijn etc)	Gedeeltelijk		50	1	50
8	2.6 Is vastgelegd welke acties onmiddellijk dienen te worden genomen bij incidenten met hoge impact (bijv. wanneer patiëntveiligheid in gevaar komt)?	Ja		100	1	100
9	2.7 Zijn van de benodigde personen, in geval van een calamiteit, bereikbaarheidsgegevens (mobiel nummer) bekend en is in het continuïteitsplan vastgelegd waar deze te vinden zijn?	Ja	Alle belangrijke telefoonnummers bij helpdesk vastgelegd	100	1	100
10	2.8 Is vastgelegd wie verantwoordelijk is voor uitvoering van de verschillende maatregelen?	Ja		100	1	100
11	2.9 Is vastgelegd wie coördinatie rondom de noodprocedures en uitwijk op zich neemt?	Ja		100	1	100
12	2.10 Hebben betrokken personen voldoende opleiding/kennis om de benodigde activiteiten te kunnen uitvoeren?	Gedeeltelijk	functioneel beheerders gaan nog op applicatiecursus	50	1	50
13	2.11 Zijn afspraken vastgelegd over hoe interne communicatie verloopt bij noodsituaties?	Ja		100	1	100
14	2.12 Zijn de gemaakte afspraken over maximale uitvalduur en servicelevels in geval van uitwijk/failover vastgelegd in de interne SLA's?	Ja		100	1	100
15	2.13 Zijn de vereiste inspanningen van externe leveranciers vastgelegd in SLA's?	Ja		100	1	100
16						
17						
18	Totaal Organisatie	88				
19						
20						
21						
22						
23						
24						
25						
1. Algemene gegevens 2. Organisatie 3. Risico- en Impactanalyse 4. Maatregelen 5. Testen 6. Onderhoud 7. Overzicht						
Gereed NUM						

Microsoft Excel - BeoordelingsInstrument_continuïteitsbeheer_0.2_ingevuld.xls						
Bestand Beveiligen Invoegen Opmaak Extra Data Venster Help						
C3 Ja						
Typ een vraag voor hulp						
A	B	C	D	E	F	G
Vraagnr	Vraag	Antwoord	Opmerkingen / Voorstel ter verbetering	Score	Gewicht	Gewogen score
2	Risicoanalyse					
3	3.1 Zijn risico's vastgesteld, die onderbreking van het bedrijfsproces kunnen veroorzaken (bijvoorbeeld: storing van apparatuur, computervirus)	Ja		100	1	100
4	3.2 Is vastgelegd welke systemen of applicaties het bedrijfsproces ondersteunen?	Ja		100	1	100
5	3.3 Is vastgesteld hoe waarschijnlijk het optreden van de genoemde risico's is?	Nee	Hebben we geen gegevens over, is moeilijk in te schatten	0	0.5	0
6	Impactanalyse					
7	3.4 Is er een impactanalyse uitgevoerd om de gevolgen van de onderbrekingen vast te stellen (in de vorm van omvang van de schade en benodigde hersteltijd)	Ja		100	1	100
8	3.5 Is vastgelegd waaruit de gevolgen van verstoring van het bedrijfsproces kunnen zijn (in termen van gevolgen voor patiënten, medewerkers, geïnvesteerde tijd, financiële gevolgen)?	Ja		100	1	100
9	3.6 Is vastgesteld welke de maximale uitvalsduur van het bedrijfsproces is? (in termen van minuten, uren, dagen)	Ja		100	1	100
10	3.7 Is vastgesteld wat het maximale toegestane verlies aan gegevens is voor het bedrijfsproces? (bijv. laatste 10 minuten, 3 uur etc)	Ja	Verlies van gegevens is in het geheel niet acceptabel	100	1	100
11						
12	Totaal Risico- en Impactanalyse	92				
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
1. Algemene gegevens / 2. Organisatie / 3. Risico- en Impactanalyse / 4. Maatregelen / 5. Testen / 6. Onderhoud / 7. Overzicht /						
Gereed NUM						

Microsoft Excel - BeoordelingsInstrument_continuïteitsbeheer_0.2_ingevuld.xls						
Bestand Bewerken Beeld invoegen Opmaak Extra Data Venster Help						
C3 Gedeeltelijk						
A	B	C	D	E	F	G
Vraagnr	Vraag	Antwoord	Opmerkingen / Voorstel ter verbetering	Score	Gewicht	Gewogen score
1	Algemeen					
3	4.1 Zijn de te nemen maatregelen/procedures tot op 'werkniveau' uitgewerkt?	Gedeeltelijk	mist nog een expliciete uitdraagprocedure voor de helpdesk	50	1	50
4	Preventieve maatregelen					
5	4.2 Zijn er fysieke maatregelen genomen ter voorkoming van uitval (bijv. afgesloten serverruimte)	Ja	Is opgenomen in de centrale infrastructuur, met beveiligd rekencentrum	100	1	100
6	4.3 Worden backups gemaakt en is externe veiligstelling hiervan geregeld?	Ja		100	1	100
7	4.4 Is vastgesteld of wijze waarop en frequentie van back-ups doeltreffend is, gezien de eisen die daaraan worden gesteld?	Ja		100	1	100
8	4.5 Zijn voor kritische systemen maatregelen getroffen om hierop binnen afgesproken tijd ondersteuning te bieden (ofwel door fysieke beschikbaarheid medewerkers, ofwel door (beveiligde) remote support voorzieningen)?	Ja		100	1	100
9	4.6 Is er sprake van uitwijkmogelijkheden (dubbel uitvoering of bijv. afspraken met hardwareleverancier over een backup-site)	Ja	alle kritische systeemdelen in 2 rekencentra	100	1	100
10	Correctieve maatregelen					
11	4.7 Zijn er noodprocedures vastgesteld voor storingen waarvoor geen uitwijk noodzakelijk is (bijv. kapotte printer)	Gedeeltelijk	Nog niet helemaal duidelijk wat te doen als bijv. monitor of printer storing heeft, wordt nu helpdesk voor gebeld	50	1	50
12	4.8 Zijn er noodprocedures uitgewerkt voor tijdelijke overbrugging wanneer de geautomatiseerde informatiesystemen zijn uitgevallen? (bijv. handmatige verwerking op papier, procedure voor opvragen labuitslagen bij lab etc.)	Ja		100	1	100
13	4.9 Is er een systeem van nood-accounts en procedures voor de inzet van deze nood-accounts? (zodat bij problemen met gebruikers accounts, er beheerst noodaccounts uitgereikt kunnen worden)	Nee	Wordt niet mee gewerkt, is misschien aandachtspunt voor toekomst	0	0,5	0
14	4.10 Is beschreven hoe een uitwijk- of failoverprocedure dient plaats te vinden?	Ja	In beheer handboek	100	1	100
15	4.11 Is vastgelegd wie verantwoordelijk is voor uitvoering van uitwijk- of failoverprocedure?	Ja		100	1	100
16	4.12 Is een zogenaamde 'uitwijkofficer' beschikbaar waarin (kopieën van) uitwijk- en terugkeerprocedures veilig bewaard kunnen worden?	Ja	In noodprocedure-ordner	100	1	100
17	4.13 Zijn afspraken met externe leveranciers gemaakt rondom reparatie, reserveonderdelen etc?	Ja		100	1	100
18	Maatregelen tbv hervatten werkzaamheden					
19	4.14 Is er een terugkeerprocedure waarin wordt beschreven welke acties dienen te worden ondernomen om de normale bedrijfsvoering te hervatten?	Nee	Is nog niet overnagedacht, punt van aandacht	0	0,5	0
20						
21	Totaal Maatregelen	85				
22						
23						
24						
1. Algemene gegevens / 2. Organisatie / 3. Risico- en Impactanalyse / 4. Maatregelen / 5. Testen / 6. Onderhoud / 7. Overzicht /						
Gereed NUM						

Microsoft Excel - BeoordelingsInstrument_continuïteitsbeheer_0.2_ingevuld.xls						
Bestand Beveiligen Invoegen Opmaak Extra Data Venster Help						
C3 Nee						
Typ een vraag voor hulp						
A	B	C	D	E	F	G
Vraagnr	Vraag	Antwoord	Opmerkingen / Voorstel ter verbetering	Score	Gewicht	Gewogen score
2	Testen maatregelen					
3	5.1 Is er een testschema opgesteld voor het continuïteitsplan?	Nee		0	1	0
4	5.2 Vindt het testen planmatig plaats? (zijn doelstellingen duidelijk, is er goede verslaglegging, vindt er evaluatie plaats)	Nee		0	1	0
5	5.3 Worden alle continuïteitsvoorzieningen hierbij getest?	Onbekend		0	1	0
6	5.4 Wordt er een rapportage ten behoeve van management opgesteld naar aanleiding van een test	Nee		0	1	0
7	5.5 Worden uitwijk- / failovervoorzieningen ten minste één maal per jaar getest?	Ja	Is opgenomen in draaiboek van beheer	100	1	100
8	5.6 Wordt getest op alle risico's uit de risico-analyse?	Gedeeltelijk		50	1	50
9						
10						
11						
12						
13	Totaal Testen	25				
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
1. Algemene gegevens / 2. Organisatie / 3. Risico- en Impactanalyse / 4. Maatregelen / 5. Testen / 6. Onderhoud / 7. Overzicht /						
Gereed NUM						

Microsoft Excel - BeoordelingsInstrument_continuïteitsbeheer_0.2_ingevuld.xls						
Bestand Bewerken Beeld Invoegen Opmaak Extra Data Venster Help						
A1 Vraagnr						
	A	B	C	D	E	F
1	Vraagnr	Vraag	Antwoord	Opmerkingen / Voorstel ter verbetering	Score	Gewicht
2	Onderhoud	continuïteitsplan				
3	6.1	Is er een onderhoudsplan beschreven waarin staat hoe en wanneer het plan wordt beoordeeld op geldigheid?	Nee		0	1
4	6.2	Is vastgelegd hoe en wanneer beoordeeld wordt of kennis en opleidingsniveau van betrokken medewerkers nog voldoende is. Wordt na wijzigingen van IT-infrastructuur, die mogelijk invloed hebben op het beschikbaarheidsniveau van de informatievoorziening, ook het continuïteitsplan bijgewerkt?	Nee		0	1
5	6.3		Gedeeltelijk	Niet standaard, is wel punt van aandacht	50	1
6						
7						
8						
9						
10		Totaal Onderhoud	17			
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
1. Algemene gegevens / 2. Organisatie / 3. Risico- en Impactanalyse / 4. Maatregelen / 5. Testen / 6. Onderhoud / 7. Overzicht /						
Gereed NUM						



Bijlage 4: Enquête validatie beoordelingsinstrument

In het kader van mijn studie 'Master of Informatics', doe ik momenteel onderzoek naar continuïteitsbeheer voor zorgkritische ICT. Met de toenemende afhankelijkheid van ICT-systemen in de patiëntenzorg is continuïteitsbeheer (ook wel Business Continuity Management) een belangrijk thema geworden.

Doel van het onderzoek is om te komen tot een beoordelingsinstrument waarmee vastgesteld kan worden of er afdoende maatregelen genomen zijn om continuïteit van de processen te waarborgen. Op basis van literatuuronderzoek en interviews binnen het UMC Utrecht zijn eisen opgesteld voor een dergelijk beoordelingsinstrument. Vervolgens zijn bestaande beoordelingsinstrumenten getoetst aan deze eisen.

Op basis van bestaande instrumenten en de verzamelde informatie heb ik een nieuw beoordelingsinstrument samengesteld. Deze kan toegepast worden bij het evalueren van continuïteitsbeheer voor bedrijfsprocessen, bijv. tijdens of na invoering van een nieuw informatiesysteem. Let wel, het gaat hier om een beoordelingsinstrument en *niet* om een continuïteitsplan. Dit instrument is niet bedoeld om de afspraken en procedures rondom het continuïteitsbeheer vast te leggen.

Graag zou ik uw mening over bruikbaarheid van dit instrument vernemen.

Het beoordelingsinstrument is in de vorm van een excel-bestand met vragen. Op het eerste tabblad staat een korte toelichting. Een ingevuld beoordelingsinstrument is als bijlage meegezonden.

- BeoordelingsInstrument_continuïteitsbeheer_ingevuld.xls

Ik zou u willen vragen deze bijlagen door te nemen en nadien de volgende vragen te beantwoorden.

- 1) Is duidelijk hoe het instrument gebruikt dient te worden?
- 2) Zijn alle vragen duidelijk? Zo nee, welke vragen hebben toelichting nodig? (*svp vraagnummer + opmerkingen in het antwoord opnemen*)
- 3) Laat de vragenlijst zich eenduidig invullen? Met andere woorden, zullen de resultaten overeenkomstig zijn als verschillende collega's deze invullen?
- 4) Geeft het beoordelingsinstrument duidelijk weer op welke aspecten continuïteitsbeheer goed en op welke onvoldoende is ingeregeld?
- 5) Geeft een ingevuld beoordelingsinstrument voldoende inzicht in de status van het continuïteitsbeheer voor het betreffende proces?
- 6) Mist u vragen of aandachtsgebieden in dit beoordelingsinstrument?

7) Heeft u verdere opmerkingen of suggesties?

Bijlage 5: Interviewvragen casestudy

Over het werken met het beoordelingsinstrument

1. Hoe verliep het invullen van het beoordelingsinstrument? Tegen welke problemen liep je aan?
2. Was het invullen van het beoordelingsinstrument efficiënt, hoeveel tijd neemt het in beslag

Over de resultaten van het beoordelingsinstrument

3. Geeft het beoordelingsinstrument een herkenbaar, realistisch en representatief beeld van de staat van continuïteitsbeheer? Op welke aspecten juist wel of juist niet?
4. Geeft het beoordelingsinstrument een beter zicht op de staat van het continuïteitsbeheer rondom het proces OK-planning
5. Zouden er op basis van het beoordelingsinstrument andere maatregelen zijn genomen of afwegingen gemaakt?
6. Zouden problemen of storingen voorkomen zijn als bij implementatie dit beoordelingsinstrument was gebruikt?