Eerste hulp bij bevoegdheden

Een patiëntvriendelijke, patiëntveilige, efficiënte inrichting van de procedure voor het uitgeven, intrekken en muteren van autorisaties

Peter Jansen Klomp &
Rogger Hazelhoff

UMCG, Functioneel- & Gegevensbeheer
Noordelijke Hogeschool Leeuwarden, Accountancy

Groningen, juli 2011

Studentenbureau UMCG

Universitair Medisch Centrum Groningen

Eerste hulp bij bevoegdheden

Een patiëntvriendelijke, patiëntveilige, efficiënte inrichting van de procedure voor het uitgeven, intrekken en muteren van autorisaties.

Groningen, juli 2011

Auteur	Peter Jansen Klomp
Studentnummer	94534
Auteur	Rogger Hazelhoff
Studentnummer	96591
Afstudeerscriptie in het kader van	AO/IC Accountancy Noordelijke Hogeschool Leeuwarden
Opdrachtgever	mw. A. Weewer Functioneel- en Gegevensbeheer, UMCG
Begeleider onderwijsinstelling	K. Poelman Accountancy Noordelijke Hogeschool Leeuwarden
Begeleider UMCG	mw. L. Evers Functioneel- en Gegevensbeheer, UMCG

ISBN 978-90-8827-099-4
NUR 786 – Accountancy en administratie
Trefw AO/IC, autorisaties, procedures, rapportages, beveiliging, standaardisatie, niet-standaardisatie.

Voorwoord

Na een periode van hard werken is dit het resultaat van ons onderzoek. De opdracht zelf was niet eenvoudig. Hierbij willen wij bureau FGB en het Wenckebach instituut bedanken dat wij bij hen hebben mogen werken aan onze scriptie.

Wij willen graag mw. Muurman en mw. Evers bedanken dat zij het vertrouwen in ons hadden voor deze opdracht. Verder voor het goede aansturen vanuit mw. Evers. Zij heeft een bepaalde visie over zaken, maar liet in dit project deze visie buiten schot waardoor het echt ons onderzoek is geworden. Waardoor wij naar de inzichten vanuit de accountancy optiek konden werken.

Mw. Evers zorgde voor goede korte lijnen met haar collega's waardoor de afspraken voor interviews snel gemaakt konden worden. Hierbij willen wij ook alle geïnterviewden bedanken voor hun medewerking die zowel noodzakelijk was voor onze scriptie als voor het gehele UMCG. Zeker de ondersteuning vanuit ICT was zeer goed.

Verder een dankwoord naar dr. Pols voor de duidelijke communicatie en het regelen van de zaken m.b.t. de aanmeldingsprocedure.

Daarnaast gaat ook een dankwoord uit richting onze begeleider vanuit de Noordelijke Hogeschool Leeuwarden, dhr. Poelman. Dhr. Poelman heeft vanuit zijn kennis en kunde ons aanwijzingen gegeven waar wij rekening mee moesten houden tijdens het uitwerken van de scriptie.

Last but not least willen wij onze opdrachtgever mw. Weewer bedanken.

Wij wensen u verder veel leesplezier en gaan er vanuit dat dit onderzoek een duidelijke inzage geeft in de bevoegdhedenprocessen van het UMCG.

Groningen, juli 2011

Peter Jansen Klomp
Rogger Hazelhoff

INHOUDSOPGAVE

SAMENVATTING

De aard van de werkzaamheden van het UMCG en de complexiteit van de organisatie maken dat informatiebeveiliging (inclusief de waarborging van de privacy) een zeer belangrijk aspect van de dagelijkse bedrijfsvoering uitmaakt. Toch bestaat er op papier geen procedure voor het uitgeven, muteren en verwijderen van bevoegdheden. Doordat de opzet, het bestaan en de werking van de procedures niet gecontroleerd kunnen worden kan er niet gesteund worden op de bevoegdheden en dus op het geautomatiseerde systeem. Dit leidt tot een onbetrouwbare informatiebeveiliging en een onbetrouwbare informatievoorziening.
Bureau Functioneel- & gegevensbeheer (FGB) verstrekte de volgende opdracht: geef advies omtrent een patiëntvriendelijke, patiëntveilige[1], efficiënte inrichting van de procedure voor het uitgeven, muteren en verwijderen van bevoegdheden bij het gebruik van UMCG-brede applicaties, ten einde:

- Duidelijkheid te scheppen voor medewerkers;
- Het proces efficiënter te laten verlopen;
- Een UMCG-brede standaardisatie te creëren als het gaat om autorisaties;
- Een meer betrouwbare informatiebeveiliging en informatievoorziening te creëren.

Het onderzoek is beperkt tot de algemene procedures rondom het uitgeven, muteren en verwijderen van bevoegdheden van de UMCG-brede applicaties: de organisatorische beveiliging.

Om de doelstelling zo volledig mogelijk te realiseren, is gebruik gemaakt van een combinatie van onderzoeksmethoden:

Secundair onderzoek: om theoretische achtergrondinformatie te verzamelen over bevoegdheden, controle, processen, organisatie en management en om UMCG-specifieke informatie over deze onderwerpen te verzamelen en relevante onderzoeken te achterhalen.

Kwalitatief onderzoek: om diepgang in het onderzoek te krijgen. Uit doelmatigheidsoverwegingen is kwalitatief onderzoek beperkt tot sleutelfiguren in de UMCG-organisatie voor wat betreft de bevoegdhedenprocessen.

Intern onderzoek: om te komen tot de huidige en gewenste situatie. De huidige situatie is vastgesteld op basis van de verzamelde onderzoeksinformatie. De vastgestelde huidige situatie is op juistheid en volledigheid besproken met sleutelfiguren. De huidige situatie is geanalyseerd op sterke en zwakke punten. De gewenste situatie is in lijn met de doelstelling en het theoretisch kader opgesteld. Om de overgang van de huidige situatie naar de gewenste situatie te bevorderen, is een veranderingsproces geformuleerd.

Conclusies:

- Door de procedure te documenteren is er duidelijkheid geschapen voor de medewerkers;
- Door de controlefunctie in te voeren worden bevoegdheden meer up-to-date gehouden;
- Dankzij de controlefunctie blijven bevoegdheden niet langer tot in lengte van dagen in de applicaties staan. Bepaalde bevoegdhedenprocessen, zoals het verwijderen van bevoegdheden, verlopen hierdoor efficiënter. Ook neemt de patiëntveiligheid hierdoor toe;
- Door het creëren van een 'Soll'-positie voor de bevoegdhedenprocessen wordt standaardisatie gecreëerd op afdelingsniveau. Standaardisatie op organisatieniveau wordt afgeraden;
- Door de controlefunctie toe te passen wordt er een **meer betrouwbare informatiebeveiliging** en **meer betrouwbare informatievoorziening** gecreëerd;

[1] De term "patiëntvriendelijk" wordt hier gedefinieerd als de vertraging die de patiënt ondervindt door de procedure. Aan "patiëntveilig" wordt de betekenis: 'waarborging van de privacy van een patiënt' toegekend.

- Ondanks dat er wijzigingen in het verloop van de bevoegdhedenprocessen zijn aangebracht, blijft de **patiëntvriendelijkheid** gewaarborgd.

Aanbevelingen:
- Een hiërarchisch leidinggevende mandateert altijd een ondergeschikte als tekenbevoegde.;
- Leidinggevenden moeten voorzien worden van een 'Soll'-positie om controle uit te kunnen oefenen op de bevoegdhedenprocessen;
- Standaardisatie biedt een aanknopingspunt voor de 'Soll'-positie van de controle, het is echter niet aan te raden voor elke afdeling. Afdelingen moeten daarom individueel en onafhankelijk van elkaar bepalen of standaardisatie voor hen de juiste methode is;
- Leidinggevenden moeten hun verantwoordelijkheid nemen en controle op de bevoegdhedenprocessen uitoefenen.

Op de volgende bladzijde bevindt zich een stappenplan voor het implementatietraject (figuur 1).

	Standaardiseren	Niet standaardiseren	Verantwoordelijk
Controle-technische functiescheiding creëren bij mandatering	•	•	ICT bevoegdhedenbeheer
Grondslag 'Soll'-positie bepalen	•	•	Hiërarchisch leidinggevende
Uniformiteit bepalen	•		Hiërarchisch leidinggevende
Lijst met standaardbevoegdheden opstellen	•		Afdelingsbreed
Lijst met standaardbevoegdheden verankeren	•		Hiërarchisch leidinggevende
Lijst van medewerkers van de afdeling bij personeelszaken van de sector opvragen	•		Hiërarchisch leidinggevende
Afspraken met personeelszaken maken over periodiek aanleveren lijst met mutatie van medewerkers	•		Hiërarchisch leidinggevende
Analyse 'Ist'-positie en 'Soll'-positie	•		Tekenbevoegde
Controle analyse	•		Hiërarchisch leidinggevende
Bijhouden zo juist en volledig mogelijke registratie		•	Hiërarchisch leidinggevende
Registratie invullen en onderhouden		•	Hiërarchisch leidinggevende
Betrouwbare rapportagestandaard met ICT afspreken	•	•	Hiërarchisch leidinggevende
Lijst met standaardbevoegdheden onderhouden	•		Hiërarchisch leidinggevende

Figuur 1 Stappenplan

1 Inleiding

Het UMCG is met ruim 10.000 werknemers de grootste werkgever van Noord-Nederland en één van de acht UMC's in heel Nederland. De aard van de werkzaamheden en de complexiteit van de organisatie maken dat informatiebeveiliging (inclusief de waarborging van de privacy) een zeer belangrijk aspect van de dagelijkse bedrijfsvoering uitmaakt.

Dit adviesrapport is geschreven in opdracht van bureau Functioneel & gegevensbeheer om het proces rondom het uitgeven, muteren en verwijderen van autorisaties:
- Efficiënter te laten verlopen
- Een UMCG-brede standaardisatie te creëren
- Meer betrouwbare informatiebeveiliging en informatievoorziening te verwezenlijken
- Ook schept het rapport meer duidelijk voor het huidige personeel, het rapport geeft immers de leidraad van de bevoegdhedenprocessen.

Het onderzoek heeft als doelstelling het adviseren van de afdeling ICT/FGB van het UMCG omtrent een patiëntvriendelijke, efficiënte inrichting van de procedure voor het uitgeven, intrekken en muteren van autorisaties bij het gebruik van UMCG-brede applicaties. De term patiëntvriendelijk wordt hierin gedefinieerd als de vertraging die de patiënt ondervindt door de bevoegdhedenprocessen.

Om de doelstelling te bereiken wordt gebruik gemaakt van een vraagstelling. De vraagstelling geldt tevens als leidraad voor de indeling van het rapport en is als volgt samengesteld:
- Wat leert de theorie ons over het toevoegen, muteren en verwijderen van autorisaties?
- Hoe ziet het (relevante) bedrijfsprofiel van het UMCG eruit?
- Hoe ziet de huidige situatie omtrent het toevoegen, muteren en verwijderen van autorisaties eruit?
- Welke knelpunten doen zich voor in de huidige situatie?
- Waarom zijn dit knelpunten?
- Hoe kunnen deze knelpunten, volgens de theorie, verholpen worden?
- Welke oplossing heeft de voorkeur?
- Hoe ziet de gewenste situatie omtrent het toevoegen, muteren en verwijderen van autorisaties eruit?
- Hoe kan de gewenste situatie bereikt worden?
- Welke conclusies kunnen worden getrokken?
- Welke aanbevelingen kunnen worden gedaan?

Omdat het UMCG een zeer grote organisatie is, met zeer veel medewerkers, afdelingen en systemen, is het onderzoek beperkt tot de procedures rondom het uitgeven, muteren en intrekken van autorisaties van de UMCG-brede applicaties.

2 Onderzoeksopzet

In dit hoofdstuk wordt de onderzoeksopzet besproken. In paragraaf 1.1 komt de aanleiding van het onderzoek aan bod waarna de probleemstelling in paragraaf 1.2 besproken wordt. In paragraaf 1.3 wordt de afbakening aangegeven waarna de methodiek van onderzoek wordt aangegeven in paragraaf 1.4. Tot slot komt in paragraaf 1.5 de analyse en rapportage.

2.1 Aanleiding

Dagelijks zijn in het UMCG duizend patiënten opgenomen, bezoekt een veelvoud daarvan een polikliniek en werken er meer dan 10.000 medewerkers samen aan zorg, onderzoek en onderwijs. Het merendeel van de medewerkers heeft één of meerdere bevoegdheden om met ondersteuning van verschillende applicaties en informatiesystemen de werkzaamheden te verrichten. [2]Daarnaast hebben alle medewerkers een UMCG-pas, om toegang te krijgen tot bepaalde delen van de gebouwen. Ook zijn ruimten beveiligd met een cijfercombinatie om ongewenste toegang tegen te gaan. Het UMCG is hiermee duidelijk een grote, complexe zorginstelling, waarbij de aard van de werkzaamheden en de complexiteit van de organisatie maken dat de informatiebeveiliging (inclusief de waarborging van de privacy) een zeer belangrijk aspect van de dagelijkse bedrijfsvoering uitmaakt.

Ondanks de omvang en complexiteit van de organisatie bestaat er op papier geen procedure voor het uitgeven, intrekken en muteren van autorisaties. Omdat onduidelijk is hoe deze procedure in werkelijkheid verloopt wordt de verantwoordelijkheid voor deze procedure door de afdelingen aan elkaars verantwoordelijkheden toegerekend. Doordat de opzet, het bestaan en de werking van de procedures niet bij alle afdelingen gecontroleerd kunnen worden, kan er niet gesteund worden op de autorisaties en dus op het geautomatiseerde systeem. Dit leidt tot onbetrouwbare informatiebeveiliging en een onbetrouwbare informatievoorziening.

Het ontbreken van een duidelijke procedure voor het uitgeven, intrekken en muteren van autorisaties leidt niet alleen bij de betrokken medewerkers tot onduidelijkheden, maar vertraagt en frustreert ook het inwerken van nieuwe medewerkers. Het lijkt alsof nieuwe medewerkers met enige regelmaat niet tijdig de juiste en volledige autorisaties hebben en hierdoor onnodig lang moeten wachten om dan eindelijk te mogen inloggen.

Hoeveel applicaties er binnen het UMCG in totaal gebruikt worden is niet bekend. Een anonieme bron bij ICT heeft aangegeven dat er 600 applicaties in beheer zijn. Daarnaast zijn er buiten het ICT om nog vele applicaties actief in het UMCG, hierop heeft het ICT geen zicht over de hoeveelheid.

Landelijk worden UMCs en ziekenhuizen geconfronteerd met budgetverlagingen voor 2011 en toenemende neerwaartse druk op de uitgaven voor gezondheidszorg, onderwijs en onderzoek in de komende jaren, het UMCG is daar geen uitzondering op. Tegengesteld aan deze tendens is dat de vraag naar zorg en de kosten van nieuwe behandelmogelijkheden almaar door blijven groeien.

[3]De maatschappelijke druk om steeds meer en meer gespecialiseerde patiëntzorg te leveren voor minder geld wordt dan ook almaar zwaarder. Hierdoor komt de nadruk steeds meer te liggen op efficiënter (doelmatiger) werken. Organisatieadviesbureau McKinsey heeft recent in opdracht van het UMCG onderzoek gedaan naar de mogelijkheden van het UMCG om efficiënter te kunnen werken en kwam met aanbevelingen:

De meeste efficiencyverbeteringen worden voor ongeveer de helft gedreven door operationele sturing en kleine proceswijzigingen;

De meeste veranderingen zullen (bijna) geen invloed hebben op de kwaliteit van de primaire processen. Wel zal op veel plekken meer standaardisatie nodig zijn om de effici-

[2] Bron: (Wenckebach Instituut)

[3] Bron: (McKinsey&company, 2011)

ency te verhogen. Dat vereist enerzijds dat gebruikers (afdelingen en artsen), accepteren dat er minder maatwerk geleverd wordt, maar kan anderzijds ook leiden tot professionelere ondersteuning (overal volgens de beste standaard). Bij een aantal functies leiden besparingen tot een verlaging van het serviceniveau (bijvoorbeeld secretariële ondersteuning).
Het realiseren van deze aanbevelingen zal echter onvermijdelijk consequenties hebben voor de interne dienstverlening en voor de mate van "maatwerk" die geleverd kan worden per sector en per afdeling.[4] In hoeverre er op het gebied van autorisaties kosten- en schaalvoordelen behaald kunnen worden is niet bekend.

2.2 Probleemstelling

Op basis van de aanleiding wordt er een probleemstelling opgesteld. Deze wordt gedefinieerd in een onderzoeksvraag en subonderzoeksvragen.

2.2.1 Onderzoeksvraag

Advies geven aan de afdeling FGB/ICT van het UMCG omtrent een patiëntvriendelijke[5], patiëntveilige[6], efficiënte inrichting van de procedure voor het uitgeven, intrekken en muteren van autorisaties bij het gebruik van UMCG-brede applicaties ten einde:

- Duidelijkheid te scheppen voor het huidige personeel;
- Efficiënter het proces te laten verlopen;
- Een UMCG-brede standaardisatie te creëren als het gaat om autorisaties;
- Een meer betrouwbare informatiebeveiliging en informatievoorziening te creëren.

Bureau FGB heeft daarbij gefungeerd als primaire opdrachtgever.

2.2.2 Subonderzoeksvragen

- Wat leert de theorie ons over het toevoegen, muteren en verwijderen van autorisaties?
- Hoe ziet het (relevante) bedrijfsprofiel van het UMCG eruit?
- Hoe ziet de huidige situatie omtrent het toevoegen, muteren en verwijderen van autorisaties eruit?
- Welke knelpunten doen zich voor in de huidige situatie?
- Waarom zijn dit knelpunten?
- Hoe kunnen deze knelpunten, volgens de theorie, verholpen worden?
- Welke oplossing heeft de voorkeur?
- Hoe ziet de gewenste situatie omtrent het toevoegen, muteren en verwijderen van autorisaties eruit?
- Hoe kan de gewenste situatie bereikt worden?
- Welke conclusies kunnen worden getrokken?
- Welke aanbevelingen kunnen worden gedaan?

2.3 Afbakening

In dit onderzoek zal worden ingegaan op de algemene procedure rondom de UMCG-brede applicaties. Een workflowmodel voor de individuele applicaties is beschikbaar bij ICT bevoegdhedenbeheer. Er bestaan naast UMCG-brede applicaties ook afdelingsspecifieke applicaties. Deze zullen niet worden onderzocht. Het onderzoek is beperkt tot de organisatorische beveiliging. De fysieke toegangsbeveiliging valt dan ook buiten de scope van dit onderzoek. Daar waar in de mannelijke vorm is geschreven, wordt verwezen naar personen van beide geslachten.

2.4 Onderzoeksmethoden

Het gebruik van slechts één onderzoeksmethode zou een te beperkt onderzoeksresultaat opleveren. Om de onderzoeksvraag zo volledig mogelijk te realiseren, is er daarom gebruik gemaakt van een combinatie van onderzoeksmethoden.

Hieronder volgt een opsomming van de gebruikte onderzoeksmethoden met een korte motivatie:

- Secundair onderzoek;
- Kwalitatief onderzoek;
- Intern onderzoek.

---

[4] Bron: (McKinsey&company, 2011)
[5] Patiëntvriendelijkheid wordt hier gedefinieerd als de vertraging die de patiënt ondervindt door de procedure
[6] Patiëntveiligheid wordt hier gedefinieerd als de waarborging van de privacy van de patiënt

2.4.1 Secundair onderzoek

Secundair onderzoek, ook wel deskresearch genoemd, is het analyseren van bestaande informatie uit verschillende informatiebronnen. Secundair onderzoek kan zeer effectief worden gebruikt om ergens gedetailleerde informatie over te verkrijgen. Bij dit onderzoek is deskresearch ingezet om theoretische achtergrondinformatie te verzamelen over bevoegdheden, controle, processen, organisatie en management en om UMCG-specifieke informatie over deze onderwerpen te verzamelen en relevante onderzoeken te achterhalen.

2.4.2 Kwalitatief onderzoek

De strategie voor informatiebepaling is vastgesteld op basis van de vier strategieën, zoals geformuleerd door Davis en Olsen[7]. Binnen dit onderzoek is de onderzoeksvraag goed te structureren, ook is er een hoog kennis- en ervaringsniveau bij de geïnterviewden aanwezig. Daarnaast is de procesonzekerheid laag, omdat alle geïnterviewden kennis- en ervaringsdeskundigen zijn. De toegepaste strategie voor informatiebepaling is daarom de Oberstrategie van Davis en Olsen.

De Oberstrategie betekent een directe ondervraging van de betrokkenen. Voor het toepassen van de Oberstrategie zijn verschillende methoden beschikbaar, de bij dit onderzoek gehanteerde methode is interviewen. De keuze voor interviewen is gemaakt, omdat de overige methoden een te oppervlakkig resultaat op zouden leveren. Daarnaast is deze methode effectiever en meer betrouwbaar. Door het interviewen te beperken tot sleutelfiguren in de UMCG-organisatie, kan op zeer efficiënte en effectieve wijze informatie bepaald worden. Sleutelfiguren zijn medewerkers die een cruciale rol hebben in het proces rondom de onderzoeksvraag. De volgende groepen sleutelfiguren zijn meegenomen in dit onderzoek:.

- Afdelingshoofden;
- Functioneel netwerkbeheerders;
- Onderzoekers van aangrenzende onderzoeken;
- Functioneel beheerders.

2.4.3 Intern onderzoek

Het resultaat van het onderzoek en de conclusie en adviezen zijn gebaseerd op het omschrijven van de gewenste situatie ('Soll'-situatie), welke is afgeleid van de geanalyseerde huidige situatie ('Ist'-situatie). De 'Ist'-situatie bestaat uit een analyse van de huidige situatie, inclusief sterke en zwakke punten (Gaps). De 'Ist'-situatie is op basis van de verzamelde onderzoeksinformatie samengesteld en met sleutelfiguren op juistheid en volledigheid doorgesproken. De 'Soll'-situatie is de gewenste situatie, waarin op beargumenteerde wijze afgeleid van de onderzoeksvraag, de Gaps worden opgeheven of tot een minimum worden beperkt. De gewenste situatie is in lijn met de doelstelling en het theoretisch kader opgesteld. Om de overgang van de 'Ist'-situatie naar de 'Soll'-situatie te bevorderen, is een veranderingsproces geformuleerd. Het veranderingsproces is gericht op het realiseren van veranderingen door elementen van de bestaande situatie aan te passen, zodat de gewenste situatie wordt bereikt.

2.5 Analyse en rapportage

De resultaten van het onderzoek zijn uitgewerkt in deze rapportage. De tussentijdse resultaten zijn gerapporteerd aan de opdrachtgever en de begeleider van het onderzoek. De resultaten zijn binnen de probleemstelling en afbakening van het onderzoek geanalyseerd.

In het volgende hoofdstuk wordt een bedrijfsbeschrijving gegeven over het ziekenhuis en wordt er ingegaan op haar taken.

[7] Bron: (Bemelmans) pagina 187, 188

3 Bedrijfsbeschrijving

In de bedrijfsbeschrijving wordt het Universitair Medisch Centrum Groningen (UMCG) weergegeven. Hier worden haar kerntaken, missie en visie weergegeven. Daarnaast wordt de organisatiestructuur weergegeven met daarbij de Raad van Bestuur en Raad van Toezicht. Tot slot wordt de geschiedenis en de huidige situatie van het UMCG behandeld.

3.1 Het UMCG

Het Universitair Medisch Centrum Groningen (UMCG) is één van de grootste ziekenhuizen in Nederland en de grootste werkgever van Noord-Nederland. De ruim 10.000 medewerkers werken in de patiëntenzorg en aan vooraanstaand wetenschappelijk onderzoek, waarbij de focus ligt op 'gezond en actief ouder worden'. Hierbij wordt In het kader van wetenschappelijk onderzoek en onderwijs nauw samen gewerkt met de Rijksuniversiteit Groningen. Er worden studenten opgeleid tot arts, tandarts of bewegingswetenschapper en artsen opgeleid tot medisch specialist. Patiënten komen in het UMCG voor basiszorg, maar ook voor zeer specialistische diagnostiek, onderzoek of behandeling. De zorg wordt gegeven door uitstekende doktoren en verpleegkundigen. Samen met ondersteunend personeel werken zij dagelijks aan die ene, gemeenschappelijke doelstelling: bouwen aan de toekomst van gezondheid.
Het UMCG wordt geleid door de Raad van Bestuur (RvB). De Raad van Toezicht is belast met het toezicht op de Raad van Bestuur. Voor de organogram zie figuur 11 in de bijlage.

3.1.1 Kerntaak: zorg

Patiënten komen in het UMCG voor 'gewone' ziekenhuiszorg, maar ook voor zeer specialistische diagnostiek, onderzoek of behandeling. Alle patiënten uit Noord-Nederland met gecompliceerde of zeldzame aandoeningen worden uiteindelijk naar het UMCG verwezen. Voor sommige zeer complexe behandelingen is het UMCG zelfs het enige ziekenhuis in Nederland. Goede zorg is altijd gebaseerd op de nieuwste inzichten. Veiligheid en kwaliteit staan daarbij voorop, vanzelfsprekend met oog voor de wensen van haar patiënten. Zorg houdt voor het UMCG niet op bij de ziekenhuismuren. Het UMCG werkt daarom nauw samen met huisartsen, verloskundigen, thuiszorg en tal van andere zorginstellingen.

3.1.2 Kerntaak: onderwijs

De Groningse opleidingen staan zeer hoog aangeschreven en bieden tal van uitdagende extra's: zo wordt de bachelor Geneeskunde ook in het Engels aangeboden en kunnen excellente geneeskundestudenten een extra opleiding volgen, die gericht is op het doen van wetenschappelijk onderzoek; de Junior Scientific Masterclass. Daarnaast bestaat de mogelijkheid om tijdens hun studie te promoveren.
In het UMCG worden ongeveer 3400 studenten per jaar opgeleid tot arts, tandarts of bewegingswetenschapper en ruim 450 artsen opgeleid tot medisch specialist. Het UMCG heeft alle opleidingen tot specialist in huis. Ook verzorgt het UMCG tal van (zorg)opleidingen op HBO- en MBO-niveau. In het kader van wetenschappelijk onderzoek en onderwijs wordt nauw samen gewerkt met de Rijksuniversiteit Groningen. Alle opleidingen zijn natuurlijk gebaseerd op de nieuwste inzichten en leiden uitstekende doktoren, verpleegkundigen en paramedici op.

3.1.3 Kerntaak: onderzoek

Het UMCG doet onderzoek naar nieuwe technieken en behandelingen, nieuwe medicijnen en nieuwe vormen van zorg waarbij de focus ligt op 'gezond en actief ouder worden'. Hierbij wordt nauw samen gewerkt met de Rijksuniversiteit Groningen. Het fundamenteel en klinisch onderzoek van het UMCG behoort tot de internationale wetenschappelijke top. De aanwezigheid van unieke biobanken en state-of-the-art onderzoeksfaciliteiten trekt wetenschappers uit de hele wereld.

3.2 Missie en visie UMCG

Een gezonde samenleving met een bevolking die tot op hoge leeftijd actief participeert. Levensbedreigende en chronische ziekten tijdig opsporen en behandelen, en nog

liever, zien te voorkomen. Het UMCG wil hieraan bijdragen en heeft daarom als missie:

Bouwen aan de toekomst van gezondheid.

Deze missie heeft een drieledige invulling:

Pionieren in onderzoek

- Vanuit het wetenschappelijk onderzoek wezenlijk bijdragen aan nieuwe kennis over gezondheid, preventie, ziekte en behandeling.
- Kennis toetsen en delen - Nieuwe kennis toetsen in de praktijk en deze op vele manieren overdragen.
- Zorgzaam voor mensen - Zorgzaam zijn voor mensen in de volle breedte: van preventie via basiszorg naar topzorg; fysiek en geestelijk; een leven lang.

3.3 Missie en visie FGB (functioneel gegevens beheer)

De visie van het FGB is erop gericht om de samenhang te verbeteren tussen de organisatie, informatievoorziening en het ICT, waarbij FGB zich vooral richt op zaken binnen het vet omlijnde gedeelte.

	Organisatie	Informatie voorziening	ICT
Strategisch	Organisatie strategie	Informatie strategie	ICT strategie
Tactisch	Organisatie management	Informatie management	ICT organisatie
Operationeel	Operatie	Functioneel beheer	ICT operatie

Figuur 2 Werkgebied bureau FGB[8]

Dit wil zij realiseren d.m.v. haar missie hierin te laten vertalen. Het FGB heeft de volgende kernwaarden voor de missie:

- Klantparticipatie
- Integraliteit
- Transparantie
- Ketengerichtheid
- Kennis van de klantprocessen
- Marktconformiteit

Dit combinerend met het motto van bureau FGB 'Op weg naar vraaggerichte ondersteuning' zal zij in de komende jaren als speerpunten voor invulling van de opdrachtgever en klanten de ingang, de communicatie en de inrichting van bureau FGB hanteren.

3.4 Missie en visie ICT

ICT levert een ondersteunende bijdrage aan de patiëntenzorg, het onderwijs en het onderzoek door het leveren van diensten en informatie met behulp van geautomatiseerde informatiesystemen en ICT-deskundigen.

De missie van de beherende onderdelen Operationele Automatisering en Netwerken is te zorgen voor het ongestoord functioneren van de geautomatiseerde centrale informatiesystemen, het leveren van de afgesproken diensten en informatie en de betrouwbare opslag van de gegevens.

Daarnaast is het streven om het technische beheer van decentrale informatiesystemen centraal te laten uitvoeren door de beherende onderdelen van ICT op basis van efficient en effectief beheer.

3.5 Geschiedenis

[9]De geschiedenis van het Universitair Medisch Centrum Groningen begint in 1797, bij de opening van het Nosocomium Academicum. De wereld en het ziekenhuis zagen er toen heel anders uit. Hier leest u de ontwikkeling van het Nosocomium Academicum tot Universitair Medisch Centrum Groningen.

3.5.1 Historie in vogelvlucht

- 1614 Oprichting Rijksuniversiteit Groningen
- 1797 Opening Nosocomium Academicum
- 1803 Opening West-Indisch Huis
- 1817 Tyfusepidemie, oprichting Stads Armen-Ziekenhuis

[8] Bron: (FGB, 2010/2013)

[9] Bron: (UMCG)

- 1852 Samengaan van Nosocomium Academicum en het Stads Armen-Ziekenhuis.
- 1889 Akkoord nieuwe ziekenhuis van het Stadsbestuur
- 1903 Opening nieuw ziekenhuis, het APSAZ
- 1932 Specialisme Oogheelkunde
- 1938 Specialisme ontwikkelt zich snel
- 1941 Specialisme Kinderkliniek
- 1947 Oprichting Thoraxcentrum Groningen
- 1957 Eerste openhartoperatie in Nederland met be hulp van de hart-longmachine in Groningen
- 1971 Nieuwe wet in werking, academische ziekenhui zen worden zelfstandig
- ± 1975 Besluit nieuw ziekenhuis op dezelfde positie
- 1997 Nieuwbouw AZG officieel geopend
- 2005 Samenvoeging AZG en Faculteit der Medische Wetenschappen

3.5.2 Het Academisch Ziekenhuis Groningen

Op 1 juli 1971 trad een nieuwe wet in werking waardoor academische ziekenhuizen zelfstandig werden. In deze wet werd de officiële taakverdeling tussen rijksuniversiteiten en de academische ziekenhuizen vastgelegd: de universiteit was verantwoordelijk voor onderzoek en onderwijs en het ziekenhuis verschafte een werkplaatsfunctie voor deze taken. Daarnaast moest het ziekenhuis zich toeleggen op patiëntenzorg en ontwikkelingsgeneeskunde. Het Algemeen Provinciaal Stads- en Academisch Ziekenhuis werd daardoor een van de universiteit losstaande rechtspersoon en kreeg een nieuwe naam: Academisch Ziekenhuis Groningen (AZG).

In de jaren zeventig kwam er een discussie op gang over een nieuw centraal ziekenhuiscomplex. Een onderdeel van die discussie was de plaats van het AZG. Andere ziekenhuizen werden aan de rand van de stad gebouwd, waar er voldoende ruimte was. Maar het Groningse gemeentebestuur besloot anders. Het nieuwe ziekenhuis moest op dezelfde plek komen.
Er werden plannen gemaakt over hoe het ziekenhuis eruit moest gaan zien: een aantal losse gebouwen, met eigen ingangen en parkeerplaatsen. In de loop van de tijd veranderden de inzichten, waardoor er een nieuw concept kwam met één ziekenhuis met één hoofdingang, één centrale receptie en overdekte binnenstraten. In 1997 werd de nieuwbouw van het AZG officieel geopend.

3.5.3 Het Universitair Medisch Centrum Groningen

Door de steeds grotere samenhang tussen academisch onderwijs, medisch wetenschappelijk onderzoek, patiëntenzorg en de opleiding tot medisch specialist was de samenvoeging van het AZG en de Faculteit der Medische Wetenschappen noodzakelijk. Noodzakelijk om met gezamenlijk beleid te kunnen investeren in de toekomst. De samenvoeging van de twee organisaties werd op 13 januari 2005 officieel bekrachtigd. Ook kreeg de nieuwe organisatie een nieuwe naam: Universitair Medisch Centrum Groningen.

3.5.4 Samenwerkingsverbanden

- Academische Huisartsenpraktijk Groningen
- Academische Werkplaats C4Youth
- Centrum voor Revalidatie
- Healthy Ageing Network Northern Netherlands (HANNN)
- HanzeVision, Academisch Refractiecentrum Groningen
- Kinder- en Jeugdpsychiatrie
- PRA International
- UMCG Ambulancezorg
- UMCG Kanker Researchfonds
- Verloskundige Stadspraktijk
- Stichting Vrienden van het UMCG

In het volgende hoofdstuk wordt de theorie behandeld die is toegepast in het onderzoek.

4 BEVEILIGING: THEORIE

Een organisatie staat niet graag voor ongewenste situaties. Bijvoorbeeld dat opeens de gegevens van het bedrijf op straat komen te liggen dan wel andere belangrijke gegevens van een bedrijf. Dit kunnen persoonlijke gegevens zijn van de medewerkers dan wel klanten, ook kan gedacht worden aan mogelijke strategische doelstellingen, iets wat de concurrentie niet te weten mag komen. Een organisatie wil haar gegevens zo goed mogelijk bewaken en dit kan op meerdere manieren.

Maar wanneer beveiligt een organisatie haar gegevens? De organisatie begint met het bepalen van het niveau van beveiligen. De mogelijkheden hiervoor worden uitgelegd in H. 4.1.1. Nadat het niveau van beveiligen is gemaakt kan er een risicoanalyse gemaakt worden.

4.1 MANAGEN VAN BEVEILIGING

Binnen de informatievoorziening nemen informatiesystemen een belangrijke plaats in. Zij leveren de informatie die nodig is en zijn daarom een essentieel object voor het nemen van beveiligingsmaatregelen. Een van de betekenissen van beveiliging is: 'voor alle kwaad behoeden'. Dit 'kwaad' bestaat uit:[10]

- Het al of niet opzettelijk onjuist handelen van mensen binnen of buiten de organisatie.
- Gebreken in instructies, applicaties, procedures, apparaten of uitrusting.
- Calamiteiten, zoals kleine en grote rampen met de hardware, software en de ruimte waarin deze geplaatst zijn.

De beveiligingsmaatregelen moeten zodanig gekozen zijn, dat voorgaand kwaad zo veel mogelijk voorkomen wordt of zo goed mogelijk wordt opgevangen. De ongelukken hebben direct effect op het functioneren van het informatiesysteem en daarmee op de hele onderneming. Beveiliging betekent dan ook het nemen van maatregelen om ervoor te zorgen dat de informatievoorziening betrouwbaar blijft.

4.1.1 MANAGEN VAN RISICO'S

De juiste maatregelen nemen om misbruik te voorkomen en eventuele calamiteiten op te vangen, vormt een deel van risicomanagement. Om te bepalen welke de maatregelen zijn die het risicomanagement behoeft, wordt een werkwijze gehanteerd.

1. Formuleren betrouwbaarheidseisen. Hierbij wordt vastgesteld wat de eisen zijn die gesteld worden aan betrouwbare informatievoorziening.
2. Vaststellen bedreigingen. Stelt vast welke de bedreigingen zijn die het informatiesysteem kunnen uitschakelen.
3. Selecteren maatregelen. Formuleer gerichte beveiligingsmaatregelen op basis van de vastgestelde betrouwbaarheidseisen.
4. Implementeren maatregelen. Veranker, op basis van het beschikbare budget, de beveiligingsmaatregelen in de onderneming.
5. Bewaken van de uitvoering. Controleer dat de maatregelen uitgevoerd worden en stel bij onvolkomenheden de maatregelen bij.

4.1.2 RISICOGEDRAG

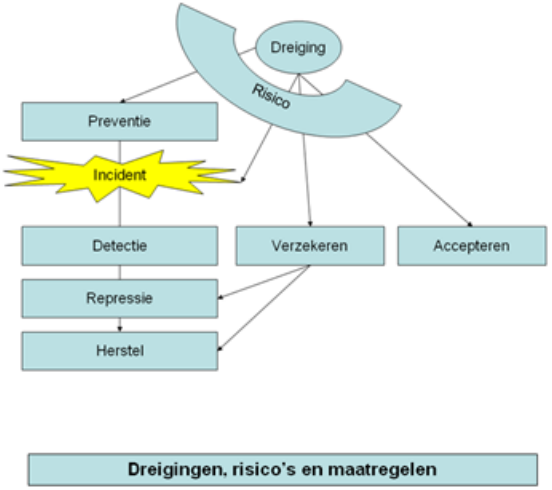
Mensen en organisaties vertonen verschillend gedrag bij het hanteren van risico's. Daarbij wordt onderscheid gemaakt tussen risicomijdend, risicodragend en risiconeutraal gedrag:

- Risicomijdend gedrag. Hierbij wordt gestreefd naar die beveiligingsmaatregelen waarmee het risico minimaal is.
- Risicodragend gedrag. Als er al maatregelen genomen worden, zijn ze reconstructief van aard.
- Risiconeutraal gedrag. In geval van risiconeutraal gedrag worden geen overmatige risico's genomen, maar worden risico's ook niet geschuwd. Beveiligingsmaat-

[10] Bron: (C.T. de Groot, 2002) H11

regelen hebben vaak een detectief of reconstructief karakter.

Figuur 3 laat een schematisch overzicht zien van risicopreventie.



Figuur 3 Risicopreventie[11]

4.2 Beveiligingsmaatregelen

Als gevolg van rampen als branden en overstromingen kan het informatiesysteem volledig uitvallen. Daarnaast kan stroomuitval, het defect raken van computers of elektronische geheugens uiterst vervelende gevolgen hebben. Een ander gevaar vormen de computervirussen. Er is een groot aantal beveiligingsmaatregelen nodig om de risico's af te dekken. Bij de beveiligingsmaatregelen behoren ook die welke het effect van calamiteiten tenietdoen.

4.2.1 Soorten beveiligingsmaatregelen

Beveilingsmaatregelen zijn op verschillende manieren in te delen. Een mogelijke indeling is de volgende:

- Preventieve maatregelen; deze hebben als doel om het optreden van verstoringen te voorkomen.
- Detectieve maatregelen; zijn gericht op het kunnen opsporen van oorzaken en gevolgen bij het optreden van verstoringen.
- Reconstructieve maatregelen; hebben de functie de gevolgen van een verstoring teniet te doen. Dit kan door:
  - Repressieve maatregelen die dienen de gevolgen van verstoringen te onderdrukken.
  - Correctieve maatregelen zijn er voor om mogelijke gevolgen van verstoringen te herstellen.

4.2.2 Werkingssfeer beveiligingsmaatregelen

Onder werkingssfeer wordt het gebied aangegeven waarop de maatregelen werkzaam zijn. Er worden drie gebieden onderscheiden:

- Logische beveiliging
- Fysieke beveiliging
- Organisatorische beveiliging

Logische beveiliging

Logische beveiliging[12] kan gezien worden als een niet-tastbare beveiliging. Het is een softwarematige beveiliging. Hierbij zijn verschillende logische beveiligingen mogelijk; zoals wachtwoorden, invoercontroles, verbandcontroles, firewall, antivirus scanners, encryptie, functiescheiding etc. Bij functiescheiding kan er gedacht worden aan primaire en secundaire functiescheiding. Primaire functiescheiding is functiescheiding tussen afdelingen en secundaire functiescheiding is functiescheiding binnen de afdeling. De maatregelen kunnen op verschillende niveaus worden ingevoerd:

- Besturingssysteem niveau
- Databasemanagementsysteem niveau
- Applicatieniveau
- Gegevensniveau; bestand, veld, record
- Mappen (directory)

De toegang van de niveaus hangt af van de autorisatie die per keer wordt uitgegeven. Mag een medewerker veel of weinig zien, doen etc.
Het belangrijkste onderdeel van de logische beveiliging is de toegangsbeveiliging.

[11] Bron: (IBpedia)

[12] Bron: (Fijneman, 2006)

De stappen die bij toegangsbeveiliging gelden zijn:
- Identificatie; wie ben je?
- Authenticatie; bewijs dat.
- Autorisatie; wat mag je?
- Logging; auditing.

Identificatie kan worden vastgesteld door een gebruikersnaam in te voeren dan wel een personeelsnummer. Deze moet overeen komen met het wachtwoord dat aan de gebruikersnaam gekoppeld is Dit is de zogenoemde authenticatie. Wanneer hierin een matching is wordt door het systeem de autorisatie gecontroleerd. Waar heeft iemand toegang tot. Is dit tot het besturingssysteem, of tot de applicaties dan wel de gegevens alleen? Daarnaast wordt in het systeem gecontroleerd welke rechten de medewerker op het bestand/in het systeem heeft. Mag deze lezen, schrijven, wijzigen, toevoegen, verwijderen, kopiëren, printen dan wel versturen?

Autorisaties worden uitgegeven aan medewerkers die in systemen, bestanden dan wel mappen moeten werken en daar bevoegdheden voor nodig hebben om toegang te krijgen. Voor het verkrijgen van de bevoegdheid zijn maatregelen genomen zodat er belangentegenstellingen komen en er controle blijft op de uitgegeven bevoegdheden. Dit wordt gekenmerkt als secundaire functiescheiding en wordt in de praktijk controle-technische functiescheiding genoemd (CTFS). Doordat in een organisatie overdracht van waarden plaatsvindt, van de ene functionaris naar een andere functionaris, ontstaat een natuurlijke belangentegenstelling tussen de onderscheiden functionarissen. Bij CTFS gaat het om 'het – waar mogelijk – voorkomen van ongewenste functiecombinaties'. Bij ongewenste functiecombinaties wordt met name gedacht aan combinaties van de beschikkende, de bewarende en de registratieve functie. Het 'waar mogelijk' houdt in dat het toepassen van een CTFS bij de structurering van een organisatie op rationele gronden moet plaatsvinden. Dit houdt in dat er een afweging gemaakt moet worden van de kosten tegen de risico's van het geen of onvolledig hebben van functiescheiding. Het doorvoeren van CTFS behoort hierdoor economisch verantwoord te zijn[13].

[13] Bron: (E.O.J. Jans, 2007) p 145-147

De logging en auditing zijn er voor calamiteiten (terughalen van gegevens) dan wel voor controle m.b.t. fraude. Hierin wordt vastgelegd wie welke handeling uitvoert (gegevens, handeling, applicatie etc.) en wanneer deze handeling wordt uitgevoerd.

FYSIEKE BEVEILIGING

Fysieke beveiliging[14] wordt gezien als het tastbaar en zichtbaar hebben van de beveiliging. Fysieke beveiligingsmaatregelen betreffen de fysieke afscherming van bijv. computerruimte, gebouw en kamers. Een bekend principe in fysieke beveiliging is het creëren van afgeschermde gebieden die alleen toegankelijk zijn voor mensen die daar voor hun taak moeten zijn. Voor de meeste bedrijven is dat niet zo heel moeilijk omdat er eenvoudig een ringenstructuur is aan te brengen: het bedrijfsterrein is afgeschermd met een hek en een slagboom. Bij de ingang zit een portier en de toegang tot de computerruimte wordt beveiligd door middel van een pasjessysteem. Voor andere bedrijven is het weer een gehele uitdaging. Neem een ziekenhuis, zoals het UMCG, waarbinnen een zekere scheiding moet worden aangebracht tussen enerzijds medische ruimten en medisch personeel en anderzijds bezoekers en wellicht patiënten.

De kenmerken van fysieke beveiliging[15] zijn het zichtbaar/opvallend zijn van de beveiliging en hierbij zijn de kosten van fysieke beveiliging relatief hoog.

ORGANISATORISCHE BEVEILIGING

Als laatste is er nog de organisatorische beveiliging. Deze beveiliging heeft te maken met procedures in een onderneming. Dit is noodzakelijk om te voorkomen dat tijdens het invoeringstraject onduidelijkheden ontstaan over de taken, verantwoordelijkheden en bevoegdheden.
Het schema van figuur 4 schetst de verantwoordelijkheden van verschillende betrokkenen in een volwassen organisatie. De aard en omvang van een organisatie bepalen of deze verantwoordelijkheden daadwerkelijk nodig zijn

[14] Bron: (Fijneman, 2006)
[15] Bron: (Fijneman, 2006)

Betrokkene	Verantwoordelijkheid
Directie	Eindverantwoordelijk, stelt informatiebeveiligingsbeleid vast en ziet toe op de uitvoering van het beleid.
Informatie-beveiligings-functionaris / Security Officer	Beheert het beleid en het normenkader, ondersteunt de implementatie van dit beleid en houdt toezicht op de algehele naleving van het beveiligingsbeleid. Heeft een onafhankelijke positie in de organisatie
Interne Audit	Toetst het stelsel van beveiligingsmaatregelen en rapporteert aan de directie.
Lijn managers	Verantwoordelijk voor de vertaling van het beveiligingsbeleid en normen naar concrete maatregelen en voor de implementatie en uitvoering van deze maatregelen binnen de desbetreffende organisatorische eenheid.
Projectleiders	Verantwoordelijk voor het opstellen en implementeren van beveiligingseisen die specifiek zijn voor het desbetreffende project.
Medewerkers	Verantwoordelijk voor alle aspecten van beveiliging met betrekking tot de functie.

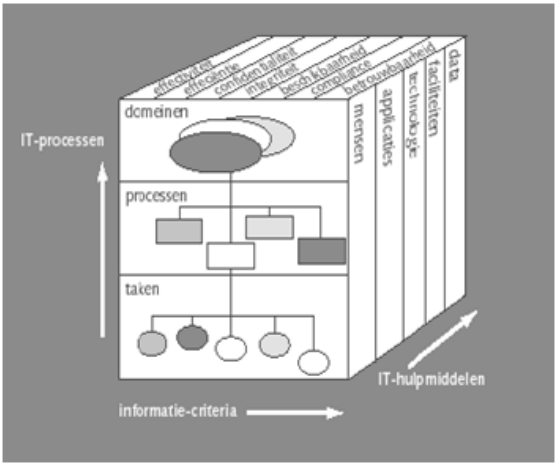
Figuur 4 Betrokkenen en hun verantwoordelijkheden[16]

Het proces informatiebeveiliging streeft ernaar om maatregelen in te richten en te onderhouden die de vertrouwelijkheid, integriteit en beschikbaarheid van informatie waarborgen.
Met beveiligingsmaatregelen kunnen de risico's die hierbij op het pad komen van een organisatie beperkt dan wel weggenomen worden. Het uitgangspunt en verreweg het belangrijkste is een goede organisatie van beveiliging, met duidelijke verantwoordelijkheden en taken, richtlijnen, rapportagelijnen en afstemming van maatregelen. De verantwoordelijkheden, bevoegdheden en taken zijn gespecificeerd ten aanzien van:

- Beleid en/of gedragrichtlijnen (welke doelstelling ten aanzien van beveiliging streven we na?)
- Processen (wat moet er gebeuren om die doelstelling te realiseren?)
- Procedures, methoden en technieken (wie doet wat, wanneer en op welke wijze?)
- Werkinstructies (hoe en wanneer worden activiteiten uitgevoerd?)

4.3 Toepassen beveiligingsmaatregelen[17]

Er is een methode ontwikkeld om alle mogelijke beveiligingsmaatregelen vast te stellen. In de methode wordt van de afhankelijkheid uitgegaan tussen de eerder behaalde kwaliteitseisen aan het informatiesysteem, de soorten beveiligingsmaatregelen en de werkingssfeer van de maatregelen. De afhankelijkheid wordt zichtbaar gemaakt in de zogeheten beveiligingskubus. De methode geeft de mogelijkheid voor een onderneming om volledigheid na te streven in de te nemen beveiligingsmaatregelen.



Figuur 5 Beveiligingskubus[18]

[16] Bron: (Fijneman, 2006)

[17] Bron: (C.T. de Groot, 2002) H11

[18] Bron: (Info over beveiligingskubus)

Om duidelijk te maken hoe de kubus werkt worden er, aan de hand van de besproken maatregelmogelijkheden in H3.2, voorbeelden gegeven.

4.3.1 Logische beveiligingsmaatregelen
- Preventief, integriteit: Inloggen
- Preventief, exclusiviteit: Codering
- Detectief, exclusiviteit: Autorisatie
- Detectief, beschikbaarheid: Audit-trail
- Detectief, beschikbaarheid: Antivirus-programma's
- Preventief, beschikbaarheid: Back-up
- Reconstructief, beschikbaarheid: Recovery
- Preventief, integriteit: Controle invoergegeven

4.3.2 Fysieke beveiligingsmaatregelen
- Preventief, exclusiviteit: Beveiliging ruimten
- Preventief, exclusiviteit: Absentiebeveiliging
- Preventief, exclusiviteit: Uitsluiten archiveringsmogelijkheden
- Preventief exclusiviteit: Afscherming datacommunicatie
- Preventief, integriteit: Raadpleegsystemen

4.3.3 Organisatorische beveiligingsmaatregelen
- Detectief, beschikbaarheid: Beveiligingsfunctionaris
- Preventief, beschikbaarheid: Systeembeheer
- Reconstructief, beschikbaarheid: Uitwijkmogelijkheden
- Preventief, beschikbaarheid: Actieplan
- Preventief, beschikbaarheid: Back-upplan

4.4 Scope

In de voorgaande paragrafen is vermeld hoe een bedrijf zijn gegevens kan beveiligen. In het kader van ons onderzoek ligt de scope niet op de gehele gegevensbeveiliging, maar vooral op de organisatorische beveiliging betreffende UMCG-brede applicaties.

4.5 Oorzaak-gevolg analyse

In hoofdstuk zes wordt gebruik gemaakt van de oorzaak-gevolg analyse. Om duidelijk te maken wat deze analyse inhoudt wordt de theorie achter de analyse besproken.

Bij een oorzaak-gevolg analyse gaat het om probleemuitingen. Er is een kernprobleem en er zijn oorzaken die dit kernprobleem veroorzaken. Problemen kunnen verward worden met risico's. De definitie van risico is; het gevaar voor schade of verlies. Een probleem staat voor; een moeilijkheid of een op te lossen vraagstuk.[19]

4.5.1 Probleemonderzoek
Het probleemonderzoek bestaat uit twee onderdelen, namelijk de probleemidentificatie en de probleemanalyse. Bij de probleemidentificatie zal het probleem moeten worden opgespoord en vastgesteld. Er is sprake van een probleem als er een afwijking ontstaat tussen de gewenste situatie, de zogenoemde norm, en de werkelijke situatie.

Normen kunnen zowel kwantitatief als kwalitatief zijn. Kwantitatieve normen zijn grootheden die aangeven de toelaatbaar geachte besteding of bereikbaar geachte prestaties. Kwalitatieve normen zijn bijvoorbeeld voorschriften, instructies en procedures die moeten worden nageleefd, respectievelijk opgevolgd. Een norm is tijd en plaats gebonden; een norm is dan ook geen statische grootheid maar een dynamische. Een norm zal dus op juistheid moeten worden getoetst en waarnodig worden herzien. Met de hier omschreven controlefunctie wordt de interne controle bedoeld.

Wanneer naar voren is gekomen dat er een bepaald probleem is, dient te worden vastgesteld wat het probleem nu precies is. In dit kader is er een bekend gezegde dat in alle situaties opgaat: 'een juist gesteld probleem is al half opgelost'.

Het is van belang dat men zich realiseert dat niet iedereen in organisaties er belang bij heeft om problemen te identificeren. Probleemontkenning en vluchtgedrag zijn in veel organisaties dan ook bekende verschijnselen. Bij het ontbreken van een duidelijke norm is het onmogelijk vast te stellen of er sprake is van afwijkingen.

Nadat vastgesteld is dat een probleem zich voordoet, dient het probleem geanalyseerd te worden (probleemanalyse). Er wordt dan stilgestaan bij de werkelijke oorzaak-en-

[19] Bron: (Over van Dale)

gevolgrelatie van het probleem. Gezocht wordt naar feiten die het probleem rechtvaardigen. Bij de laatste opmerking komt het regelmatig voor dat problemen inschattingen van personen zijn ten aanzien van bepaalde ontwikkelingen. Met dit subjectieve element dient voorzichtig mee te worden omgegaan.

Vragen die binnen deze fase gesteld kunnen worden zijn:
- Is het probleem incidenteel of structureel?
- Hoe urgent is het probleem?
- Wat is de reikwijdte van het probleem?
- Wat is de relatie van het probleem met andere afdelingen binnen en buiten de organisatie?
- Is het probleem rationeel of organisatorisch van aard? 20

Uit de analyse zal moeten blijken wat de oorzaken zijn geweest die tot de geconstateerde afwijkingen hebben geleid. Op grond van deze kennis kunnen maatregelen worden getroffen om in de toekomst soortgelijke afwijkingen te voorkomen. In een later stadium zal moeten worden nagegaan in hoeverre de correctieve maatregelen effect hebben gehad.

Afwijkingen tussen het bereikte en het gewenste resultaat behoeven niet altijd het gevolg te zijn van een onjuiste of minder correcte uitvoering, ook het gestelde doel – het gewenste resultaat – kan in de gegeven omstandigheden niet reëel zijn. Wanneer het verwezenlijken van een doelstelling onrealistisch is of door omstandigheden onhaalbaar is geworden, zal de doelstelling moeten worden 'bijgesteld'. De controlefunctie is geëvolueerd tot wat in de Angelsaksische literatuur wordt aangeduid met 'control' Het controlproces omvat dan controle-, analyse- correctie- en evaluatieactiviteiten. [21]

4.5.2 Wat is 'control'
In feite houdt control in: het onder controle houden – het beheersen – door managers van activiteiten die in de organisatie onder ieders verantwoordelijkheid plaatsvinden. Dit geldt zowel voor het topmanagement als voor de procesmanagers en dan niet alleen voor wat betreft de primaire processen maar ook voor de ondersteunende, de secundaire processen. Voor procesmanagement gaat het om het realiseren van concreet gestelde procesdoelen, veelal uitgedrukt in kwantitatieve en/of kwalitatieve normen, beter bekend als procesindicatoren. Daarnaast

spelen ook andere factoren een rol die van invloed kunnen zijn op een optimaal procesresultaat zoals teamgeest, motivatie medewerkers, arbeidsomstandigheden, zorg ten aanzien van beschikbaar gestelde of nodig geachte middelen.

Control van de bedrijfsprocessen is van het grootste belang voor het functioneren van organisaties. Het is namelijk pas mogelijk met de organisatie in te spelen op (te verwachten) ontwikkelingen in de samenleving wanneer de interne processen worden beheerst. Voorwaarde voor het besturen van een organisatie is dan ook dat de organisatie zelf goed functioneert.
De centrale plaats die de beheersingsproblematiek in het functioneren van organisaties inneemt heeft in de achterliggende jaren steeds meer aandacht gekregen. Hierbij mag gewezen worden op bijvoorbeeld:
- Het COSO-rapport Internal Control
- De ISO 9000-certificering
- De Balanced Scorecard
- De Corprate Governance

Hierbij is een tendens waarneembaar: organisaties moeten kunnen beschikken over een gestructureerd systeem van beheersingsmaatregelen. Deze maatregelen leiden tot controlactiviteiten waarbij het management ervoor moet zorg dragen dat ook de kwaliteit van de controlprocessen wordt beheerst.[22]

4.5.3 Organiseren van activiteiten
Om in-control te komen moeten de activiteiten van een organisatie goed worden georganiseerd. Enerzijds zal bij het organiseren van activiteiten rekening gehouden moeten worden met de externe afstemmingen van de organisatie. Kennende als de DESTEP punten. Deze staan voor:
- Demografisch
- Economisch

[20] Bron: (N. Van Dam, 2005) p 286-287
[21] Bron: (E.O.J. Jans, 2007) p 48-49
[22] Bron: (E.O.J. Jans, 2007) 50-51

- Sociaal
- Technologisch
- Ecologisch
- Politiek

Daarnaast moet gelet worden op de interne afstemming tussen individuele werknemers, machines en andere hulpmiddelen. Deze dienen onderling op elkaar afgestemd te worden. Hierbij gaat het vooral om zaken als het op gang brengen van processen en het sturen van de dagelijkse werkzaamheden. Ter verduidelijking is figuur 6 hieronder weergegeven.

Figuur 6 De tweezijdige invloed op het organiseren van activiteiten

In een organisatie wordt ook rekening gehouden met de personele structuur. Bij het vaststellen van de personele structuur wordt aandacht besteed aan:

- Hiërarchische verhoudingen, door wie worden opdrachten gegeven?
- Bevoegdheden, wie mag bepaalde beslissingen nemen?
- Personele bezettingen, welke medewerker(s) zijn werkzaam op bepaalde afdelingen en in welke functies?
- Communicatie, wie informeert anderen en op welke wijze?

De arbeidsverdeling die hierbij komt kijken kan in twee optieken worden gezien. Arbeidsverdeling in verticale richting. Hierin kan gezien worden het opstellen van een onderzoek door de hiërarchische leidinggevende en dat de opdracht wordt overgedragen naar de werknemers. Maar arbeid kan om meerdere reden worden onderverdeeld:

- Kostenmotief, taken moeten op een zodanige wijze worden ingedeeld dat een efficiënt functioneren en produceren mogelijk gemaakt wordt.
- Bestuurmotief, de wijze waarop taken opgebouwd en verdeeld worden, moet besturing van de organisatie mogelijk maken.
- Sociaal motief, taken moeten voor individuele personen een bepaalde aantrekkelijkheid bezitten.
- Maatschappelijk motief, bij de opbouw van taken moet rekening worden gehouden met de maatschappelijke eisen, bijvoorbeeld veiligheidsvoorschriften.

Wanneer taken, bevoegdheden en verantwoordelijkheden opgesplitst worden binnen een zelfde hiërarchisch niveau kan worden gesproken over arbeidsverdeling in horizontale richting. Wanneer alleen taken, zonder bepaalde bevoegdheden en verantwoordelijkheden, worden overgedragen, ontstaat een situatie waarbij het lager niveau alleen een uitvoerend karakter heeft.

Figuur 7 Verschillende graden van delegeren

Het hogere niveau neemt alle beslissingen. Het lager niveau kan in dat geval echter nooit (volledig) verantwoordelijk worden gesteld voor de uitvoering van de taak, omdat elke beslissingsbevoegdheid tot sturen hier ontbreekt. Het lager niveau kan pas verantwoordelijk worden gesteld voor de uitvoering van de taak, wanneer het een

bepaalde ruimte krijgt voor het nemen van beslissingen. Wanneer taken met de daarbij benodigde bevoegdheden en verantwoordelijkheden worden overgedragen spreekt met van delegeren van taken. Er is bij delegeren geen sprake van geheel of helemaal niet delegeren, maar er kunnen verschillende niveaus worden onderscheiden, zie figuur 7[23]

4.5.4 Beheersing van activiteiten

In H.4.5.2 werd gesproken over het beheersen van het functioneren van de organisatie. Naast de beheersing van de activiteiten kan er ook gekeken worden naar het omspanningsvermogen van de leidinggevende. Door delegatie worden taken met de daarbij behorende verantwoordelijkheden en bevoegdheden overgedragen aan lagere niveaus. Degene die de taken delegeert behoudt daarbij de eindverantwoordelijkheid voor die taken. Om ervoor te zorgen dat de gedelegeerde taken naar behoren worden uitgevoerd zal leiding moeten worden gegeven aan degenen aan wie taken gedelegeerd zijn. De vraag hierbij is aan hoeveel ondergeschikten een leider effectief leiding kan gegeven Dat aantal wordt in de theorie het omspanningsvermogen van de leider genoemd. Wanneer een leider aan teveel onderschikten leiding geeft ontstaat een situatie, waarbij er te weinig tijd is om de activiteiten af te stemmen en om stil te staan bij de kwaliteit van de uitvoering van de activiteiten door zijn ondergeschikten. Met omspanningsvermogen zijn er altijd twee dimensies aanwezig:

- De horizontale dimensie; het aantal direct ondergeschikten aan wie een leider leiding geeft, dit wordt de spanwijdte genoemd.
- De verticale dimensie; dit is het aantal niveau waaraan (in)direct leiding wordt gegeven. Dit wordt spandiepte genoemd.

De grootte van het omspanningsvermogen wordt hoofdzakelijk door de volgende factoren bepaald:

- De aard van de leider
- De aard van de medewerkers
- De aard van de organisatie
- De aard van het werk
- Het karakter van het werk

Wanneer zich een situatie voordoet kan op verschillende manier naar een oplossing worden gezocht:

- Meer delegatie van taken, met daarbij behorende verantwoordelijkheden en bevoegdheden aan het onderliggende niveau.
- Het toevoegen van een assistent-manager.
- Het toevoegen van een persoonlijke assistent aan de leider.
- Het inschakelen van andere organen in de organisatie, zoals stafdiensten.24

Bij het delegeren van taken dienen niet alle verantwoordelijkheden en bevoegdheden te worden overgedragen van een hoger niveau naar een lager niveau. Bij delegatie is het van belang dat taken, bevoegdheden en verantwoordelijkheden per functie met elkaar in evenwicht blijven. Als men delegeert, blijft de leiding verantwoordelijk voor de taak waarvoor zij is aangesteld, al verricht zij de werkzaamheden niet zelf. Voor de uitvoering van deze taken zijn de personen binnen het lagere niveau verantwoordelijk. De leiding zal controle op het lagere niveau willen uitvoeren.

4.6 Probleemanalyse

In H.4.5 is de oorzaak gevolg analyse besproken in het kader van de organisatie intern en extern. In het kader van de probleemanalyse wordt er gekeken naar de systemen. Een organisatie heeft een visie en een missie. Deze wil zij graag halen en wel zo effectief en efficiënt mogelijk.[25]

4.6.1 Vaststellen

In een organisatie loopt nooit alles volgens het boekje; bijv. de processen lopen niet volgens het boekje en de kosten stijgen. Dit kan worden beoordeeld doordat budgetten worden overschreden en een proces ver voorbij de vooraf gestelde tijdsduur gaat. Hieruit kunnen probleemgebieden

[23] Bron: (N. Van Dam, 2005) p 398-409

[24] Bron: (N. Van Dam, 2005) p. 409-411

[25] Born: (C.T. de Groot, 2002) H3

worden vastgesteld. Belangrijk bij het vaststellen van de problemen is dat 'valkuilen' worden vermeden. De 'valkuilen' die het best vermeden kunnen worden zijn:
- Bagatelliseren van het probleem. Het probleem wordt onvoldoende onderkend, waardoor de noodzaak tot verbetering nauwelijks op gang komt.
- Voorbarige conclusies. Trek niet te snel een conclusie, of denk niet te snel de goede oplossing te weten. Neem tijd zodat bepaalde informatie niet over het hoofd wordt gezien of verkeerd wordt gebruikt.
- Probleem is alleen een mening. Let op of het probleem zich presenteert als een feit, of dat dit probleem een mening van iemand is.
- Probleem afschuiven. Door te doen alsof het niet jouw probleem is, hoef je het ook niet op te lossen.

4.6.2 Verkenning

De eerste stap van het probleemoplossingproces bestaat uit het verkennen van het probleem. Wordt een probleem niet als zodanig herkend of erkend, dan is het oplossen van dat probleem niet relevant. Niemand zal immers bereid zijn te investeren in een oplossing van een niet-herkend of niet-erkend probleem. 'Een probleem dat iemand als probleem ziet, is géén probleem'.

Problemen zijn te herkennen aan de probleemuitingen; dat zijn signalen vanuit de organisatie waar iets als ongewenst wordt ervaren. De probleemuitingen zullen als eerste geïnventariseerd moeten worden.

4.6.3 Analyse

Bij de analyse wordt de bron van de probleemuiting vastgesteld en het probleem herleidt tot de probleemkern. Ook is het nodig om na te gaan aan wie het probleem kan worden toegeschreven: de probleemeigenaar wordt bepaald.

De probleemeigenaar is een persoon, afdeling of onderneming die schade zal ondervinden bij het voortduren van het probleem. De probleemeigenaar wil inspanning verricht om het probleem opgelost te krijgen.

4.6.4 Formuleren

Probleemuitingen zijn vaak te herleiden tot één oorzaak. Het vaststellen van de probleemkern. De oorzaak van de probleemuitingen wordt de probleemkern genoemd. Is de probleemkern niet duidelijk te formuleren, dan wordt een probleem beschouwinggebied aangegeven. Is de kern van het probleem bepaald, dan is meestal meteen de richting uitgezet waarin de oplossing van het probleem gezocht moet worden.

4.6.5 Oplossingsalternatieven

Bij het opstellen van oplossingen voor het probleem is het verstandig om meerdere mogelijke oplossingen in kaart te zetten. Dit om de vraag te kunnen stellen, welke oplossing is het beste voor het gestelde probleem.

4.6.6 Haalbaarheid

Nadat er een aantal oplossingen zijn bepaald zal er een haalbaarheidsonderzoek verricht moeten worden. Bij het haalbaarheidsonderzoek van de gekozen oplossingsalternatieven wordt vastgesteld op basis van de:
- Technisch haalbaarheid
- Operationele haalbaarheid
- Economische haalbaarheid.

Bij de technische haalbaarheid wordt vastgesteld of de noodzakelijke hard- en software in huis aanwezig is of dat de middelen beschikbaar zijn voor de aanschaf ervan.

Onder operationele haalbaarheid wordt verstaan in hoeverre men binnen en buiten de organisatie bereid is aan het gekozen alternatief mee te willen werken. Dit impliceert dat de toekomstige gebruikers aantoonbaar baat moeten hebben bij het werken met het gekozen oplossingsalternatief. Voor de bepaling van de operationele haalbaarheid moet het volgende worden nagegaan:
- Mensen
  - Heeft de oplossingen gevolgen voor de werkgelegenheid?
  - Wat is de bereidheid van de medewerkers om op de nieuwe manier te werken?
- Werkwijze
  - Moeten als gevolg van de introductie van de nieuwe werkwijze de taken aangepast worden?
  - Vereist de nieuwe werkwijze een grote discipline tijden het toepassen?

- Omgeving
    - Welke gevolgen hebben de voorgestelde interne veranderingen voor de kwaliteit van de dienstverlening?
    - Is er intensere samenwerking nodig met de omgeving?

Met economische haalbaarheid wordt bedoeld dat de kosten of investeringen in het gekozen oplossingsalternatief op moeten wegen tegen de verwachte opbrengsten. Voor de economische haalbaarheid wordt het volgende nagegaan:
- Kosten/baten
    - Wat zijn de investeringskosten voor de aanschaf van de eventueel benodigde hardware?
    - Wat zijn de kosten voor aanschaf of voor ontwikkeling van de software?
    - Hoeveel bedragen de complementaire kosten, zoals kosten voor onderhoud en beheer?
    - Zijn er meer of minder medewerkers nodig?
- Management
    - Wordt de verandering gesteund door het management?

4.6.7 Keuze

Na de technische, operationele en economische haalbaarheid met elkaar vergeleken te hebben wordt er een keuze gemaakt voor het alternatief dat hoogstwaarschijnlijk het best gaat functioneren in de organisatie.

4.6.8 Opdracht

Na de keuze wordt de projectopdracht opgesteld. Hierbij wordt een projectleider aangesteld die een projectplan schrijft. Een projectopdracht geeft nauwkeurig aan wat er van het project verwacht wordt. De projectgroep weet op basis hiervan wat er te doen staat en het management weet waarvoor het toestemming geeft.

Een projectopdracht omvat:
- Een doel. De doelstelling van de probleemeigenaar wordt hier geformuleerd.
- Een resultaat. Kort wordt aangegeven wat het resultaat moet worden van het project.
- Beperkingen. Aangegeven wordt wat de beperkende voorwaarden zijn om de verbetering te realiseren zoals tijd, geld en beschikbare mensen.

4.7 Standaardisatie

Aan het begin van dit hoofdstuk spraken we over beveiligen. Wanneer neemt een organisatie actie tot beveiligen en welke mogelijkheden zijn daarvoor? Verder is er gesproken over het achterhalen van problemen en waarmee daarbij rekening gehouden moet worden. Alles draait hierbij om het goed in stand houden van de 'Soll'-positie. (Uitleg H4) Maar hoe krijgt een afdeling van een organisatie deze positief op een zo'n effectief en efficiënt mogelijke manier? Dit kan aan de hand van standaardisatie. Maar wat is standaardisatie?[26]

Standaardisatie kan worden gedefinieerd en beleefd als uniformiteit in het uitvoeren van procedures. Om het beheer van een systeem te vergemakkelijken is standaardisatie belangrijk. Hoe groter en hoe complexer het informatiesysteem, des te belangrijker standaardisatie wordt. Standaardisatie is belangrijk bij alle beheertaken.

Enkele voorbeelden van standaardisatie zijn:
- In applicaties en in het besturingssysteem worden zoveel mogelijk dezelfde instellingen voor alle gebruikers gehanteerd.
- Werkstations in het informatiesysteem worden zoveel mogelijk uitgerust met dezelfde hardware. Zo weten systeembeheerders wat er in elke computer zit, wat belangrijk kan zijn bij het oplossen van problemen.
- Handleidingen en andere documenten hebben zoveel mogelijk dezelfde indeling.
- Gegevens worden op dezelfde manier in dezelfde structuur opgeslagen, zodat ze snel gevonden kunnen worden.
- Regels en procedures zijn zoveel mogelijk gelijk voor alle afdelingen en mensen, zodat iedereen weet wat wel en niet mag.

[26] (Instruct online)

Voordelen van standaardisatie zijn:
- Het is gemakkelijker om het systeem en de instellingen te leren kennen. Hierdoor kunnen problemen gemakkelijker opgespoord worden en nieuwe medewerkers sneller ingewerkt worden.
- Documentatie, programma's en dergelijke hebben dezelfde indeling, waardoor het gemakkelijker is om ze te lezen of ermee te werken.
- Door een heldere gestandaardiseerde structuur is het gemakkelijker om later onderdelen aan het systeem toe te voegen en om gegevens voor verschillende doelen te gebruiken.

Nadelen van standaardisatie zijn:
- Gebruikers moeten de regels en procedures kennen en deze naleven. Dat werkt alleen goed als gebruikers daar ook toe bereid zijn. Daarom moeten ze voorgelicht worden over de redenen van standaardisatie.
- Soms doen gebruikers iets allang op een voor hen logische manier. Als ze dan volgens nieuwe standaardisatieregels moeten werken, duurt hun werk langer en dat zal weerstand oproepen.
- Soms kan een taak van een gebruiker veel gemakkelijker uitgevoerd worden als van de standaard afgestapt wordt. Het kan nodig zijn om bepaalde instellingen aan te passen of om speciale applicaties op een computer te installeren. Daarbij moet gestreefd worden naar zoveel mogelijk standaardisatie, maar moet ook worden bedacht dat het systeem er is om gebruikers zo goed mogelijk in hun werk te ondersteunen.

Nu duidelijk is geworden wat standaardisatie inhoudt zijn er nog verschillende standaardisatie mogelijkheden. Kennende:
- De functiestandaardisatie
- Het autorisatieproces standaardisatie

4.7.1 Functiestandaardisatie
Functiestandaardisatie houdt in dat functies in een organisatie gelijk aan elkaar worden. Voorbeeld hiervan is dat alle verpleegkundigen op een afdeling dezelfde bevoegdheden krijgen naar aanleiding van hun functie en niet naar aanleiding wat zij denken te mogen. Het beoordelen van de functies en deze functies te koppelen in het systeem, kan, afhankelijk van de afdeling, zeer lang duren. Wanneer de functies eenmaal in het systeem zitten kan het aanvragen van autorisaties passend bij de functie zeer snel gebeuren.

4.7.2 Autorisatieproces standaardisatie
Bij autorisatieproces standaardisatie gaat het om het proces van aanvragen dat voor iedere afdeling gelijk is. Zo is er voor een organisatie een uniform in aanvragen zodat het voor iedereen duidelijk is hoe de aanvragen verlopen.

4.8 Succesfactoren
Om de beoogde veranderingen naar een geslaagd proces te leiden zijn de volgende voorwaarden van cruciaal belang: [27]
- Zorg voor voldoende draagvlak. Het overgrote deel van de medewerkers in een organisatie is bereid om mee te denken over, en mee te werken aan, veranderingen wanneer voor hen duidelijk is dat de noodzaak daartoe bestaat. De eerste voorwaarde voor het slagen van de omslag is dus gelegen in het informeren en overtuigen van de medewerkers van de noodzaak ervan. Laat zien wat de veranderingen beogen en draag zorg voor een brede vorm van participatie van verschillende afdelingen en diensten in dit traject. Medewerkers worden daardoor medeverantwoordelijk voor het eindresultaat.
- Zorg voor geplande verandering. Een veranderingsproces is succesvol wanneer er sprake is van voldoende sturing. Laat medewerkers zien welke doelen gehaald dienen te worden en binnen welk tijdsbestek. Betrek ze bij de uitwerking van de doelen. Zorg dat die doelen voldoende uitdagend zijn om mensen in beweging te krijgen, maar bewaak tegelijkertijd de haalbaarheid ervan. Niets is immers zo demotiverend dan het najagen van schimmen. Programmeer de veranderingen in een vrij strak schema, dit om de vaart erin te houden en te voorkomen dat er teveel detailleringen worden aangebracht.
- Zorg voor een integrale aanpak. Betrek alle relevante diensten en afdelingen van de zorgorganisatie bij dit veranderingsproces om te zorgen dat er betrokkenheid is met het proces en zij zich daar niet tegen af gaan zetten. Informeer tijdens het veranderingsproces een ie-

[27] Bron: (Succesfactoren)

der actief. Proeftuinen dienen in het algemeen vermeden te worden.
- Stel randvoorwaarden. Verandering geschiedt topdown zowel wat betreft inhoud als proces. Binnen deze kaders kan inhoudelijk een bottum-up ontwerp gemaakt worden.
- Ontwerp op hoofdlijnen. Bij het ontwerpen van veranderingen dient het ontwerp in de eerste fase beperkt te blijven tot hoofdlijnen. Ontwerp een “casco”, waarbinnen later, met en door medewerkers zelf, nadere detailleringen aan te brengen zijn.
- Neem snelle, korte stappen. Deel het veranderproces in een aantal stappen in, die voor de medewerkers te behappen zijn.
- Zorg voor onomkeerbaarheid. Zorg steeds dat een bepaalde fase of stap met een duidelijk besluit wordt afgerond. Dit onderstreept de ernst waarmee de veranderingen worden aangepakt of doorgevoerd en voorkomt dat er steeds weer terug wordt gekomen op discussies die al eerder gevoerd zijn. Stel geen besluiten uit; in een veranderingstraject zijn immers de kool en de geit niet altijd te sparen. Besluit op basis van wat goed is en niet op basis van wat goed valt.
- Zorg voor een goede projectorganisatie. Bij het ontwerpen en invoeren van (ingrijpende) veranderingsprocessen, is het verstandig om een projectorganisatie -bijvoorbeeld stuurgroep en werkgroepen- in te stellen met een daarbij behorende besluitkracht. Zorg wel voor een goede afstemming met de reguliere lijnorganisatie.
- Neem voldoende afstand. Leidinggevenden/uitvoerenden hebben zich vaak de normen en waarden van de organisatie eigen gemaakt. Problemen en daaraan gekoppelde oplossingsrichtingen worden vanuit dat kader geformuleerd. In een veranderingstraject is het van groot belang dat met name het management afstand neemt en probeert buiten het eigen kader te treden ('thinking aside').

In het volgende hoofdstuk worden de bedrijfsspecifieke begrippen behandeld. Dit zodat de huidige situatie met haar afkortingen begrijpelijk wordt.

5 Bedrijfs-specifieke begrippen

Omdat er veel gebruik wordt gemaakt van functiebenamingen dan wel afkortingen, wordt in dit hoofdstuk toegelicht waar ze voor staan dan wel wat ze doen.

5.1 Tekenbevoegde

De tekenbevoegde is de medewerker die het recht heeft om medewerkers te autoriseren. De tekenbevoegde krijgt van een hiërarchische leidinggevende de bevoegdheid om autorisaties toe te kennen aan medewerkers via het IDS/ISS systeem. De bevoegdheid wordt verstrekt via een mandatering die door de hiërarchische leidinggevende kan worden aangevraagd dan wel door een ondergeschikte medewerker. Alleen door de hiërarchische leidinggevende kan deze mandatering worden ondertekend. Het zijn van een tekenbevoegde is geen functie, het wordt omschreven als een taak naast de eigen functie van de medewerker waar een aantal uren voor staat.

5.2 Functioneel netwerkbeheerder: tekenbevoegde +

De functioneel netwerkbeheerder wordt in dit rapport vermeld als een FNB'er. Bij de FNB'er komen alle aanvragen binnen voor autorisaties van medewerkers van de betreffende afdeling. Het proces gaat verder precies zoals het bij de tekenbevoegde gaat. Daarnaast kan de FNB'er een tekenbevoegde+ zijn. De + houdt in dat dit persoon aanspreekpunt is voor de gehele ICT afdeling. Dit kan gaan over updates nieuwe software, nieuwe hardware etc. Dit om de processen tussen de afdelingen te verbeteren.

5.3 Tekenbevoegde +

In hoofdstuk vier wordt gesproken over tekenbevoegde+, dit zijn de besproken functies in 5.1 en 5.2 gezamenlijk.

5.4 Ketenvoorzitter

Een keten ontstaat door de aaneenschakeling of ordening van processen van verschillende afdelingen die gericht zijn op het gezamenlijk bereiken van het vooraf vastgestelde doel. Hierbij houdt de voorzitter in de gaten of het doel ook wordt behaald en niet wordt voorbijgestreefd door overige activiteiten. De ketenvoorzitter kan gezien worden als een hiërarchische leidinggevende.

5.5 Functioneel leidinggevende

De functie van functioneel leidinggevende zit op hetzelfde niveau in de organisatie als de medewerkers. Deze geeft leiding aan hen en rapporteert alle gehaalde resultaten aan de hiërarchische leidinggevende.

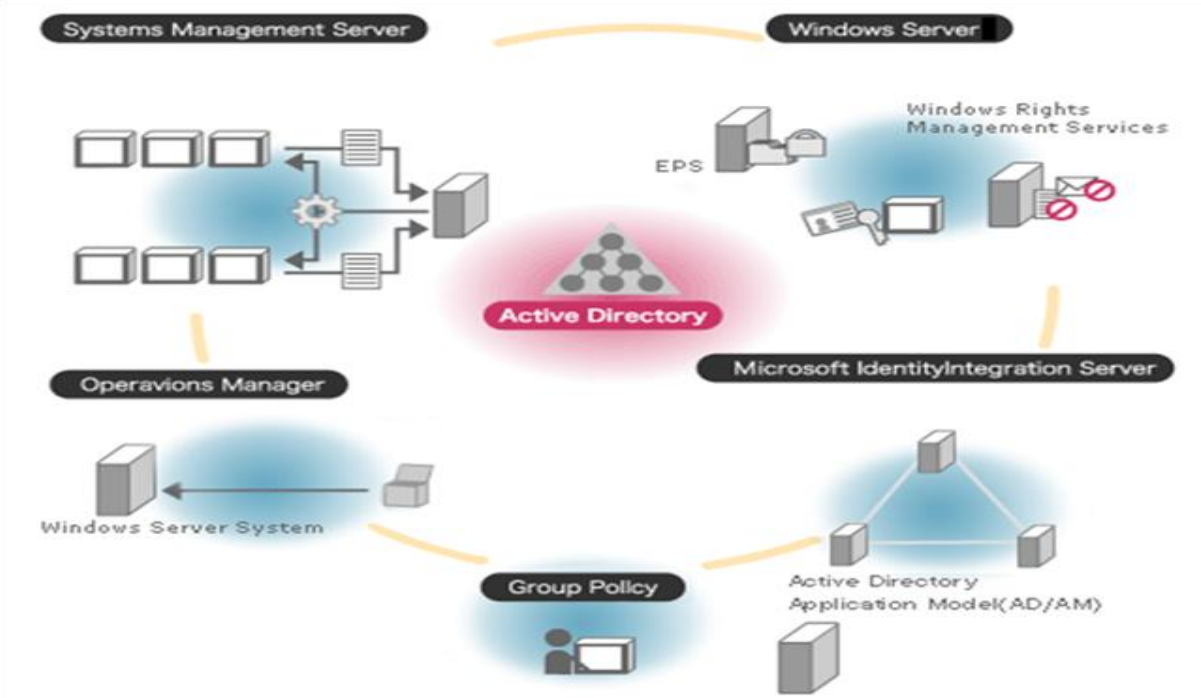
5.6 Hiërarchisch leidinggevende

De hiërarchisch leidinggevende zit t.o.v. de functioneel leidinggevende hoger in het organogram van de organisatie. Deze persoon ontvangt alle resultaten van de functioneel leidinggevenden en bepaalt het doel wat de hiërarchisch leidinggevende wil behalen in de toekomst.

5.7 IDS

IDS staat voor ICT Digital Service. Met deze webapplicatie kunnen de door afdelingen aangestelde medewerkers bevoegdheden aanvragen voor gebruikers van ICT producten en diensten. Door middel van digitale formulieren worden de aanvragen verwerkt door de ICT Helplijn en teruggekoppeld per e-mail naar de aanvrager. IDS is bereikbaar via het intranet, wanneer men bevoegd is om IDS te gebruiken kan men d.m.v. een inlogscherm de website benaderen. [28] IDS controleert niet of een medewerker onder de mandatering van de tekenbevoegde valt.

[28] Bron: Informatie via P.J. van der Veen ontvangen



Figuur 7 Active Directory[29]

5.8 ISS

Het ISS staat voor ICT Self Service. Dit is een nieuw systeem waarmee de aanvragen voor autorisaties sneller kunnen worden verwerkt. Van het ISS systeem maakt, evenals het IDS, alleen de FNB'er gebruik. Dankzij ISS hoeft de aanvraag niet meer te worden gecontroleerd en geautoriseerd door ICT bevoegdhedenbeheer. Dit komt doordat het ISS controleert of de aanvraag daadwerkelijk door een FNB'er wordt ingevoerd. Doordat de aanvraag nu automatisch door het systeem wordt gecontroleerd, wordt de aanvraag direct uitgevoerd en is de autorisatie ook direct actief. Zoals in het IDS moet ook in het ISS het personeelsnummer worden ingevoerd voordat de aanvraag kan worden uitgevoerd. Daarnaast hoeft een accountaanvraag niet meer via ICT bevoegdhedenbeheer te gaan, dit kan via ISS zelf gereageld worden. Hier kan eveneens een aanpassing zelf door de FNB'er worden uitgevoerd en kan er een einddatum voor het account worden ingevoerd.

5.9 AD

Het AD staat voor Active Directory. AD is een eigen implementatie door Microsoft. AD staat beheerders toe om het netwerk van een volledig bedrijf te beheren. De instellingen van de AD worden centraal opgeslagen in een database. Een Active Directory kan worden gedefinieerd als een hiërarchische structuur en deze structuur is meestal onderverdeeld in drie hoofdcategorieën; de middelen zoals hardware en printers, diensten voor eindgebruikers, zoals web-e-mailservers en de voorwerpen die de belangrijkste

[29] Bron: (Tech-FAQ, Info over Active Directory)

functies van het domein en netwerk bewerkstelligen. [30] Zie ook figuur 8.

5.10 ADS

Het ADS staat voor Active Directory System. Dit systeem is nagenoeg gelijk als het AD. Alle gegevens komen tezamen in een grote database en personen die voor deze database geautoriseerd zijn kunnen daaruit de benodigde informatie halen.

5.11 ZIS

Het ZIS staat voor het Ziekenhuis Informatie Systeem en is een elektronisch informatiesysteem. Het systeem bevat o.a. patiëntgegevens en het beheer van de administratieve patiëntgegevens, biedt ondersteuning aan het logistiek zorgproces en biedt ondersteuning aan het facturatie proces.

5.12 Bevoegdhedenpatroon

Het bevoegdhedenpatroon heeft betrekking op het recht hebben van bevoegdheden bij een bepaalde functie. Zo heeft iedereen met dezelfde functie ook recht op de basis bevoegdheden die daarbij horen.

5.13 Ketens

De aaneenschakeling of ordening van parallelle processen van verschillende bedrijfsonderdelen, gericht op het gezamenlijk bereiken van een vastgestelde doelstelling. Bedrijfsonderdelen werken samen aan producten en diensten die in de keten worden geleverd.[31]

5.14 Peoplesoft

Peoplesoft is het personen- en personeels-informatiesysteem voor het UMCG. In Peoplesoft worden van alle medewerkers de benodigde gegevens vastgelegd voor o.a.:

- Het correct kunnen betalen van de maandelijkse salarissen.
- De ziektemelding en de voortgang in het herstel worden geregistreerd ten einde een goede begeleiding van de medewerker door de leidinggevende mogelijk te maken
- De keuzes voor verhoogd en extra persoonlijk budget registreren.
- Het kunnen vervaardigen van overzichten zoals de Norm en Standlijst, een actueel ziekte overzicht, het maken van RPF'en (rechtspositieformulieren) etc.[32]

5.15 BEVPER

BEVPER is een systeem dat er voor zorgt dat er een koppeling komt tussen het microsectienummer van een medewerker en het personeelsnummer van dezelfde medewerker. Zodat wanneer een aanpassing gemaakt wordt in het ZIS account deze direct ook gekoppeld wordt aan het personeelsaccount.

5.16 Microsectienummer

Het microsectienummer is het nummer waaronder de medewerker in het ZIS geregistreerd staat.

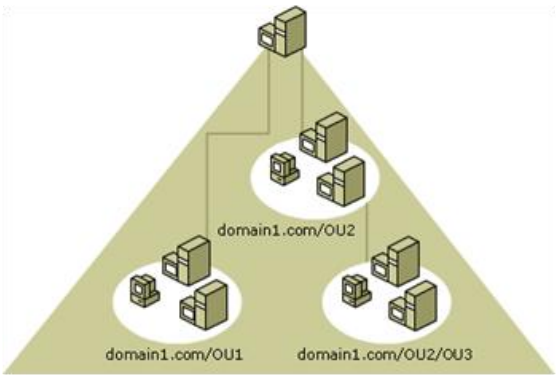
5.17 OU

OU staat voor Organizational Unit. Een OU zijn AD containers waarin men gebruikers, groepen, computers en andere organisatorische eenheden kan plaatsen. Een OU kan geen objecten uit andere domeinen bevatten. Een OU is de kleinste eenheid waarin men het beleid van een groep kan instellen. Met behulp van OU kan men 'containers' binnen een domein vestigen. Deze staan voor de hiërarchische en logische structurering in de organisatie.

Zoals weergegeven in figuur 9, kan een OU meerdere OU's bevatten. Als het nodig is kan de hiërarchie van een container worden uitgebreid. Met behulp van OU's zullen het

[30] Bron: (Tech-FAQ, Info over Active Directory)
[31] Bron: (Info over ketens)
[32] Bron: (Info over PeopleSoft)

aantal domeinen dat nodig is in de organisatie geminimaliseerd worden.[33]



Figuur 8 Orgizational Unit [34]

5.18 'Ist'-situatie

Met de 'ist'-situatie wordt de huidige situatie bedoeld. Hiermee wordt geduid hoe de procedure op dit moment loopt voor het verstrekken, muteren en verwijderen van bevoegdheden en de controle die hierop wordt uitgevoerd.

5.19 'Soll'-situatie

Met de 'Soll'-situatie wordt de gewenste situatie bedoeld. Hoe de procedures er volgens het boekje uit zou moeten zien om 'in control' te zijn met je procedure voor het uitgeven, muteren en verwijderen van bevoegdheden.
De in dit hoofdstuk vermelde begrippen komen ter sprake in de processen beschreven in het volgende hoofdstuk.

5.20 Vegasuite

Vegasuite is een programma dat alle aanvragen via IDS en ISS opslaat. Vanuit Vegasuite kunnen rapportages wordt opgevraagd, bijvoorbeeld wie welke bevoegdheid heeft. Vegasuite was in gebruik tot 18 mei.

5.21 Clientèle

Clientèle is de opvolger van Vegasuite. Tot 18 mei liep deze gezamenlijk met Vegasuite, na 18 mei is Clientèle het enige systeem dat de aanvragen opslaat.

Nu de termen zijn besproken volgt in het volgende hoofdstuk de huidige situatie.

[33] Bron: (Info over Organizational Unit)
[34] Bron: (Info over Organizational Unit)

6 HUIDIGE SITUATIE

In dit hoofdstuk wordt de vastgestelde huidige situatie beschreven van het UMCG met betrekking tot het uitgeven, muteren en verwijderen van de bevoegdheden. Voor de methode waarop de huidige situatie tot stand is gekomen wordt verwezen naar hoofdstuk 2.

In de bijlage treft u de huidige situatie in een procesbeschrijving. Deze is weergegeven in het blauw, de in het geel gekleurde toevoegingen daarbij duiden op de gewenste positie.

Het hoofdstuk bestaat uit:
- De tekenbevoegde
- Het verstrekken van bevoegdheden voor medewerkers van de eigen afdeling
- Het verstrekken van bevoegdheden voor medewerkers buiten de eigen afdeling
- Het uitbreiden, muteren van bevoegdheden
- Het intrekken van bevoegdheden als een medewerker extern vertrekt.

6.1 DE TEKENBEVOEGDE

Het bevoegdhedenproces begint met het aanstellen van een tekenbevoegde. Een afdeling bepaalt naar eigen inzicht hoeveel medewerkers de taak tekenbevoegden naast hun eigen functie krijgen. Hierbij maken de medewerkers zelf de keuze of zij tekenbevoegde willen zijn.

1) De hiërarchisch leidinggevende mandateert zichzelf of een ondergeschikte als tekenbevoegde.
2) De mandatering wordt via de interne post naar ICT bevoegdhedenbeer opgestuurd.
3) ICT bevoegdhedenbeheer controleert de mandatering op juistheid en volledigheid.
4) Na de controle van ICT bevoegdhedenbeheer zijn er meerdere mogelijkheden voor de vervolg actie:
   a) Een afgekeurde mandatering gaat, met motivatie, retour naar de afzender
   b) Op de goedgekeurde mandatering staat vermeld dat de oude tekenbevoegde moet worden verwijderd. Deze handeling wordt eerst uitgevoerd voordat de mandatering wordt uitgevoerd.
   c) De mandatering wordt uitgevoerd.

Vervolg op 4b/4c

5) ICT bevoegdhedenbeheer documenteert de mandatering in ringbandmappen en scant deze (in de loop van de tijd) in. Tevens houden zij een eigen registratie in Excel bij.
6) De medewerker is tekenbevoegd.

De tekenbevoegde kan nu bevoegdheden aanvragen via IDS/ISS voor de medewerkers. De tekenbevoegden hebben ook als enigen toegang tot deze systemen

Voor processchema zie figuur 12 in de bijlage.

6.2 HET VERSTREKKEN VAN BEVOEGDHEDEN VOOR MEDEWERKERS VAN DE EIGEN AFDELING

Omdat niet voor iedere afdeling dezelfde handeling geldt, wordt deze paragraaf onderverdeeld in subparagrafen. Deze zijn:
- Financiële afdeling
- Verpleegafdeling
- Beheerafdeling
- Algemeen vervolg

Op al deze afdelingen worden bevoegdheden op individueel niveau verstrekt, met uitzondering van de ZIS-profielen (Ziekenhuis Informatie Systeem) en de AD (Active Directory). Bevoegdheden worden niet in een centrale applicatie ingetrokken en niet in een centrale applicatie uitgegeven.

6.2.1 FINANCIËLE AFDELING

1) Een medewerker constateert dat hij geen bevoegdheden heeft voor een bepaalde handeling.

2) De medewerker dient een verzoek in bij de hiërarchische leidinggevende van de afdeling.
3) De hiërarchische leidinggevende bepaalt of de bevoegdheden functioneel zijn voor de mede-werker voor het uitvoeren van de functie.
4) Na de bepaling van de functionaliteit zijn twee opties mogelijk:
    a) De aanvraag is functioneel en de bevoegdheid wordt aangevraagd.
    b) De aanvraag is niet functioneel en de medewerker krijgt geen bevoegdheid.

6.2.2 VERPLEEGAFDELING

1) Periodiek ontvangt de tekenbevoegde de lijst met nieuwe medewerkers van afdeling Personeels-zaken.
2) De tekenbevoegde vraagt, op basis van de functie die vermeld staat op de ontvangen lijst, de bevoegdheden tijdig aan via IDS.

6.2.3 BEHEERAFDELING

1) Een nieuwe medewerker op de afdeling.
2) De hiërarchische leidinggevende van de afdeling geeft opdracht aan de tekenbevoegde om bevoegdheden aan te vragen voor de nieuwe medewerker.

6.2.4 ALGEMEEN VERVOLG

1) De aanvraag voor bevoegdheden kan via twee manieren worden ingevoerd, dit kan via:
    a) ISS, waarna de geauthentiseerde aanvraag direct actief is.
    b) IDS, deze aanvragen komen bij ICT bevoegdhedenbeheer terecht.
2) De tekenbevoegde slaat een kopie van de aanvraag op in een, met andere tekenbevoegde van de afdeling, gedeelde map.

De aanvragen die via deze systemen lopen werden tot 18 mei opgeslagen in Vegasuit en vanaf 18 mei gebeurt dat in Clientèle.

Wanneer de aanvragen via ISS verlopen is daarmee het algemeen vervolg beëindigd. Voert de tekenbevoegde de aanvragen via IDS in dan volgt daarop het volgende proces:

3) De tekenbevoegde kan in IDS een gedeblokkeerde datum kiezen voor het afhandelen van de aanvraag. Dit omdat ICT bevoegdhedenbeheer een maximale verwerkingstermijn van vijf dagen hanteert.
4) ICT bevoegdhedenbeheer controleert handmatig of de aanvraag onder de mandatering van de tekenbevoegde valt.
5) Na de controle zijn er twee keuzes voor het vervolgproces:
    a) Afkeuring wanneer de aanvraag niet onder de mandatering valt.
    b) Goedkeuring wanneer de aanvraag onder de mandatering valt.

AFKEURING

6) Na de afkeuring wordt Vegasuit/Clientèle bijgewerkt.
7) Er wordt door ICT bevoegdhedenbeer terugkoppeling gegeven aan de aanvrager.

GOEDKEURING

6) Na de goedkeuring wordt Vegasuit/Clientèle bijgewerkt.
7) Wanneer de aanvraag onder de mandatering valt controleert ICT bevoegdhedenbeheer of zij de aanvraag zelf kunnen uitoefenen.
    a) ICT bevoegdhedenbeheer kan de aanvraag zelf uitvoeren.
    b) ICT bevoegdhedenbeheer kan de aanvraag niet zelf uitvoeren en deze wordt doorgestuurd naar de juiste medewerker van afdeling ICT en bureau FGB.

Omdat het een zeer gecompliceerd proces is wordt eerst ingegaan op het proces van 7a. ICT bevoegdheden kan de aanvraag zelf uitvoeren.

ZELF UITVOEREN

Bij de aanvraag voor bevoegdheden kan tevens de aanvraag voor een account bijgevoegd zijn.

GEEN ACCOUNT AANVRAGEN

8) De aanvraag voor de bevoegdheden wordt door ICT bevoegdhedenbeheer uitgevoerd.
9) Na uitvoering van de aanvraag wordt er een terugkoppeling gegeven aan de FNB'er van de betreffende afdeling.
10) De desbetreffende medewerker is bevoegd.

ACCOUNT AANVRAGEN

8) ICT bevoegdheden controleert of de medewerker bestaat en of aan deze medewerker reeds is verstrekt.
9) Na deze procedure zijn er drie mogelijkheden aanwezig:
    a) De medewerker wordt niet gevonden via het ADS. Hierbij stopt ook direct het proces voor het aanvragen van bevoegdheden.
    b) Medewerker wordt in het ADS gevonden maar er is nog geen account uitgegeven.
    c) Medewerker wordt in het ADS gevonden en er is ook al een account uitgegeven.

10) Vervolg actie op 9)b en 9)c zijn:
    b) Het aanmaken van een account voor de medewerker.
    c) Het actief maken van het account voor de medewerker in overleg met de afdeling waarvoor het account was uitgegeven en was gevestigd.
11) De aanvraag voor de bevoegdheden wordt door ICT bevoegdhedenbeheer uitgevoerd
12) Na uitvoering van de aanvraag wordt er een terugkoppeling gegeven aan de FNB'er van de betreffende afdeling.
13) De desbetreffende medewerker is bevoegd.

DOORSTUREN

8) De aanvraag is voor een medewerker van een bepaalde afdeling; bureau FGB dan wel afdeling ICT controleert of deze aanvraag gebruikelijk is voor de bepaalde bevoegdheid.

AANVRAAG GEBRUIKELIJK

9) De aanvraag wordt door bureau FGB dan wel afdeling ICT uitgevoerd.
10) Na het uitvoeren van de aanvraag wordt er terugkoppeling gegeven aan de tekenbevoegde.
11) De medewerker is bevoegd voor de aangevraagde bevoegdheid.

AANVRAAG NIET GEBRUIKELIJK

8) Na het afkeuren proberen de uitvoerende medewerkers informatie in te winnen bij de desbetreffende tekenbevoegde die de aanvraag heeft ingediend.
9) Nadat er informatie is verkregen zijn er twee mogelijkheden voor het vervolg:
    a) Afkeuring van de aanvraag en de aangevraagde tekenbevoegde krijgt een terugkoppeling
    b) Goedkeuring, de uitvoerende medewerkers van bureau FGB en afdeling ICT voeren de aanvraag uit.
10) Na het uitvoeren van de aanvraag wordt er terugkoppeling gegeven aan de tekenbevoegde.
11) De medewerker is bevoegd voor de aangevraagde bevoegdheid.

De hiërarchische leidinggevende van een afdeling houdt geen documentatie bij van de verstrekte bevoegdheden.

Voor processchema zie figuur 13 t/m 17 in de bijlage.

6.3 HET VERSTREKKEN VAN BEVOEGDHEDEN VOOR MEDEWERKERS BUITEN DE EIGEN AFDELING

1) Een medewerker van buiten de eigen afdeling vraagt bevoegdheden aan bij de tekenbevoegde, bij het verzoek dient deze een motivatie in te dienen.
2) De tekenbevoegde beoordeelt het verzoek en heeft twee mogelijke keuzes:
    a) Afkeuring van het verzoek en het proces wordt daarmee beëindigd.
    b) Het verzoek is voldoende, het proces gaat verder.
3) De tekenbevoegde controleert de aanvraag altijd bij de functioneel leidinggevende van de aanvragende medewerker. Deze oordeelt het volgende:
    a) Het verzoek is functioneel.
    b) Het verzoek is niet functioneel.

6.3.1 FUNCTIONEEL

4) Na goedkeuring van de leidinggevende vraagt de tekenbevoegde de aanvraag aan volgens de procedure die beschreven is in H. 6.2.4.

6.3.2 NIET FUNCTIONEEL

4) De tekenbevoegde voert de aanvraag niet uit, waarna de volgende momenten kunnen ontstaan:
    a) De medewerker protesteert niet en accepteert het feit dat hij de bevoegdheden niet kan krijgen. Hiermee stopt het proces.
    b) De medewerker is het niet eens met het besluit en stelt een brief op, aan de RvB gericht.

5) Na het ontvangen van de brief door het RvB namens de medewerker besluit het RvB het volgende:
    a) Het verzoek van de medewerker wordt afgekeurd, waarna het proces definitief stopt.
    b) Het verzoek wordt goedgekeurd en de bevoegdheid moet door de tekenbevoegde worden aangevraagd. De aanvraag gaat volgens de procedure die beschreven is in H.6.2.4.

Voor processchema zie figuur 18 in de bijlage.

6.4 Het uitbreiden/muteren van bevoegdheden

Omdat niet voor iedere afdeling dezelfde handeling geldt, wordt deze paragraaf onderverdeeld in subparagrafen. Deze zijn:
- Financiële afdeling
- Verpleegafdeling
- Beheerafdeling

6.4.1 Financiële afdeling

1) Een medewerker constateert dat deze niet bevoegdheden heeft voor bepaalde handelingen.
2) De medewerker dient een verzoek in bij de hiërarchische leidinggevende van de afdeling.
3) De hiërarchische leidinggevende beoordeelt het verzoek van de medewerker op functionaliteit en heeft twee mogelijkheden:
    a) Het verzoek is niet functioneel en de hiërarchische leidinggevende verwerpt het verzoek. Hierbij beëindigt de aanvraag.
    b) Het verzoek is functioneel, dan geeft de hiërarchische leidinggevende opdracht aan de tekenbevoegde om de bevoegdheden aan te vragen.
4) De tekenbevoegde voert de opdracht uit en vraagt de bevoegdheden aan volgens het proces dat beschreven is in H. 6.2.4.

6.4.2 Verpleegafdeling

1) Een medewerker constateert dat deze niet bevoegdheden heeft voor bepaalde handelingen.
2) De medewerker dient een verzoek in bij de tekenbevoegde van de afdeling inclusief motivatie.
3) De tekenbevoegde beoordeelt het verzoek inclusief motivatie en hierin kunnen de volgende keuzes worden gemaakt:
    a) Afkeuring, het verzoek wordt niet goedgekeurd waarna het proces eindigt.
    b) Goedkeuring, het verzoek wordt goedgekeurd waarna de aanvraag wordt uitgevoerd. De aanvraag gaat volgens de procedure die beschreven is in H.6.2.4.

6.4.3 Beheerafdeling

1) Een medewerker constateert dat deze niet bevoegdheden heeft voor bepaalde handelingen
2) De medewerker dient een verzoek in bij de tekenbevoegde van de afdeling.
3) De tekenbevoegde beoordeelt het verzoek naar redelijkheid waarna er twee mogelijkheden zijn:
    a) Het verzoek ligt niet binnen de redelijkheid en het verzoek wordt niet uitgevoerd. Hierbij stopt het proces.
    b) Het verzoek ligt binnen de redelijkheid en het aanvraag proces gaat verder.
4) Indien de aanvraag binnen de redelijkheid ligt wordt door de tekenbevoegde gekeken naar de kosten van de aanvraag. De mogelijkheid bestaat dat deze boven het maximale bedrag van de tekenbevoegde komen. Komen de kosten van de aanvraag boven het maximale bedrag:
    a) Nee, de tekenbevoegde vraagt de bevoegdheden aan volgens het proces dat is genoemd in H.6.2.4.
    b) Ja, de tekenbevoegde vraagt de aanvraag nog niet aan maar neemt contact op met de hiërarchische leidinggevende.
5) De hiërarchische leidinggevende beoordeelt de aanvraag naar functionaliteit. Hierdoor ontstaat er twee mogelijke keuzes:
    a) De aanvraag is niet functioneel, de aanvraag wordt niet uitgevoerd en hierbij stopt het proces.
    b) Het verzoek is functioneel, de hiërarchische leidinggevende geeft terugkoppeling aan de tekenbevoegde.
6) De tekenbevoegde voert de aanvraag uit volgens de procedure die is beschreven is in H.6.2.4.

Voor processchema zie figuur 19 en 20 in de bijlage.

6.5 Het intrekken van bevoegdheden als een medewerker extern vertrekt

Bij het intrekken van bevoegdheden als een medewerker extern vertrekt zijn er twee zaken die moeten worden verwijderd: het gebruikers account en de bevoegdheden. Eerst wordt het proces besproken over verwijderen van accounts, daarna het verwijderen van bevoegdheden.

6.5.1 Het verwijderen van gebruikers accounts

1) Een medewerker vertrekt extern.
2) Een medewerker van personeelszaken controleert of de vertrekkend medewerker een Peoplesoft account heeft.
    a) De vertrekkend medewerker beschikt niet over Peolplesoft account.
    b) De vertrekkend medewerker beschikt over een Peoplesoft account en een micro-sectienummer.
    c) De vertrekkend medewerker beschikt over een Peoplesoft account, maar geen micro-sectienummer.

Iedere persoon die voor het UMCG werkt heeft een ZIS-account nodig om de functie uit te kunnen voeren. Dit kunnen interne medewerkers dan wel externe medewerkers zijn. Interne medewerkers staan op de loonlijst van het UMCG en daardoor komen zij ook in het Peoplesoft systeem. Met het Peoplesoft systeem is het mogelijk om een koppeling te maken met het ZIS systeem. Externe medewerkers ontvangen geen loon van het UMCG en staan daardoor niet in het Peoplesoft systeem. De externe medewerker heeft daardoor ook geen Peolplesoft account.

6.5.2 Geen account

3) De medewerker van personeelszaken koppelt een einddatum aan het ZIS-account van de vertrekkend medewerker.
4) ICT bevoegdheden koppelt een vervaldatum aan het ZIS-account van de medewerker.
5) Het ZIS controleert tijdens het inloggen op de ontslagdatum of vervaldatum en geeft dertig dagen voor de einddatum een melding.
6) Inloggen blijft tot achtenveertig dagen na einddatum mogelijk, de melding voor vervaldatum wordt continu weer gegeven. Na achtenzeventig dagen de melding te hebben gehad, wordt het account definitief verwijderd. Dit gebeurt automatisch door het systeem. Hierna is het gebruikersaccount verwijderd.

6.5.3 Wel een account en een microsectienummer

3) De medewerker van personeelszaken koppelt de ontslagdatum aan het Peoplesoft account.
4) De medewerker die in Peoplesoft geregistreerd staat heeft een personeelsnummer. Dit nummer is via een elementnummer gekoppeld aan een microsectienummer in het ZIS, waardoor de einddatum ook in het ZIS-account wordt ingevuld. Hierbij is dit proces beëindigd.

6.5.4 Wel een account maar geen microsectienummer

3) De medewerker van personeelszaken koppelt de ontslagdatum aan het Peoplesoft account.
4) ICT bevoegdheden beheer kan via een toegestane workaround een medewerker toegang geven tot het ZIS. Zij koppelt het microsectienummer aan het personeelsnummer van de vertrekkend medewerker en voegt de medewerker toe in BEVPER. Deze gebruiker heet in het ZIS 'toekomstige ZIS gebruiker'.

Wanneer de medewerker nog niet is verwijderd bestaat er de kans op de volgende procedure.

5) Het microsectienummer van een medewerker wordt later alsnog bekend. ICT bevoegdhedenbeheer zorgt via een batch voor de koppeling tussen naam en usernummer.

Deze procedure zal in de toekomst automatisch worden gesynchroniseerd.
Het kan voorkomen dat dit proces niet wordt gestart, terwijl de medewerker niet meer werkzaam is in het UMCG. Hiervoor heeft het UMCG een script dat automatisch controleert op niet-gebruikte gebruikeraccounts in het AD. De procedure voor de AD loopt als volgt:

1) Wanneer een account langer dan een half jaar niet wordt gebruikt wordt het account geblokkeerd in de OU.
2) Wanneer het account in de OU komt heeft deze 30 dagen om weer actief te worden. Dit kan d.m.v. een helpdesk call. De volgende procedures kunnen volgen:

a) Het account staat langer dan dertig dagen in de OU. Hierdoor wordt het account automatisch verwijderd.
b) Het account staat minder dan dertig dagen in de OU.

3) De mogelijkheid is nog aanwezig om het account te activeren. Dit hangt af of er een helpdesk call komt.
a) De call komt niet, er worden geen handelingen verder uitgevoerd.
b) De call komt, het account wordt geheractiveerd en teruggeplaatst naar de medewerker.

Behalve dat de accounts van de vertrekkend medewerker moet worden verwijderd, moeten ook alle bevoegdheden van de medewerker worden verwijderd.

6.5.5 Verwijderen van bevoegdheden

1) Een medewerker vertrekt extern
2) De hiërarchisch leidinggevende denkt niet vanzelfsprekend aan het intrekken van bevoegdheden als een medewerker vertrekt. Hierdoor bestaat in de procedure een tweedeling.
a) De hiërarchische leidinggevende meldt het vertrek niet aan de tekenbevoegde waardoor de bevoegdheden in het systeem blijven bestaan en het proces staakt. In H.6.5.1 wordt gemeld welke actie het AD dan neemt.
b) De hiërarchische leidinggevende meldt het vertrek aan de tekenbevoegde.
3) De tekenbevoegde verwijdert de bevoegdheden van de medewerker.

Voor processchema zie figuur 21 en 23 in de bijlage.

6.6 Het intrekken van bevoegdheden als een medewerker intern vertrekt

Het intrekken van bevoegdheden als een medewerker intern vertrekt geschiedt op twee afdelingen; de 'oude' afdeling en de nieuwe afdeling. In deze paragraaf worden beiden besproken, beginnende met de 'oude' afdeling.

6.6.1 De 'oude' afdeling

1) Een medewerker vertrekt intern.
2) Een hiërarchische leidinggevende moet opdracht geven aan de tekenbevoegde om de bevoegdheden in te trekken. Doordat de hiërarchische leidinggevende hier veelal niet aan denkt bestaan er twee procedure mogelijkheden:
a) Het niet-melden aan de tekenbevoegden van de afdeling waardoor de bevoegdheden blijven bestaan. Hierbij is het proces ook ten einde.
b) Het melden aan de tekenbevoegde van de afdeling.
3) Wanneer de tekenbevoegde wel een melding krijgt is geconstateerd dat de bevoegdheden dan niet altijd worden ingetrokken. De volgende acties kan de tekenbevoegde ondernemen:
a) Het intrekken van bevoegdheden via IDS/ISS.
b) Het verwijderen van het gehele account, waadoor ICT bevoegdhedenbeheer denkt dat de werknemer extern vertrekt.
c) Het niet intrekken van de bevoegdheden waardoor deze blijven bestaan.

6.6.2 De nieuwe afdeling

1) Een nieuwe medewerker komt op de afdeling.
2) De tekenbevoegde krijgt een melding en vraagt bevoegdheden en een gebruikersaccount aan via IDS/ISS.
3) De aanvraag komt bij ICT bevoegdhedenbeheer en zij controleert de gebruiker via ADS. Hierbij zijn twee mogelijkheden voor het vervolg van de procedure:
a) De gebruiker bestaat niet, waardoor ICT bevoegdhedenbeheer geen actie onderneemt en het proces staakt.
b) De gebruiker bestaat en het account is verwijderd. Zie H.6.6.1 2)b.
4) ICT bevoegdheden heractiveert het bestaande gebruikersaccount en verwijdert alle rechten van applicaties en rechten van de afdeling waarvoor het account geblokkeerd was en waarvoor het account bevoegdheden had en activeert nieuwe bevoegdheden.
5) De medewerker is na deze procedure bevoegd.

Wordt een account niet verwijderd en bevoegdheden niet ingetrokken, dan heeft een medewerker voor beide afdelingen bevoegdheden.
Voor processchema zie figuur 24 in de bijlage.

6.7 Periodieke controle op de verstrekte bevoegdheden

Nadat de bevoegdheden zijn uitgegeven, wordt er vanuit de afdeling nooit controle op de verstrekte bevoegdheden uitgevoerd.

Als onderdeel van de procescontroles kijkt team Audit naar de bevoegdheden in de systemen en op papier. Deze onderdelen zijn salarissen, voorraden, inkopen, bouw, apotheek en een deel van de omzet in het kader van diagnosebehandelcombinaties.

Op sommige afdelingen verstrekt de secretaresse personeelszaken aan de tekenbevoegde eens per kwartaal een lijst van intern/extern vertrokken medewerkers. De tekenbevoegde controleert samen met de secretaresse personeelszaken eens per jaar of inderdaad alle bevoegdheden van de vertrokken medewerkers ingetrokken zijn.

De tekenbevoegde kan dit controleren door een overzicht te krijgen uit Vegasuit dan wel Clientèle. Hiertoe heeft de tekenbevoegde direct toegang, mocht dit niet zo zijn dan kan de tekenbevoegde informeren bij ICT support.

In het volgende hoofdstuk wordt de probleemanalyse behandeld.

7 Probleemanalyse

De informatie die nodig was om de huidige situatie te kunnen beschrijven werd verschaft door de gehouden interviews. Gedurende het houden van de interviews kwamen de risico's en problemen naar voren. Hierbij is een verdeling gemaakt in de risico's en problemen die significant zijn voor dit onderzoek en betrekking hebben op de doelstelling. Op basis van de genoemde theorie in H4.1 is er een inschatting gemaakt over de significante risico's en waardoor de risico's ontstaan; het probleem. Hierbij is de oorzaak-gevolg analyse uitgevoerd zoals deze is besproken in H4.5 en een probleemanalyse gebruikt volgens H4.6.
In dit hoofdstuk wordt per proces beschreven of er een probleem aanwezig is dat significant is voor het UMCG in het kader van de doelstelling.

7.1 De tekenbevoegde

Een hiërarchische leidinggevende kan zichzelf dan wel een medewerker van de afdeling mandateren voor tekenbevoegde. Kijkende naar de theorie in H4.2.2 over de controletechnische functiescheiding (CTFS) is dit een probleem omdat de hiërarchische leidinggevende dan zowel de beschikkende als de registrerende rol zou uitvoeren. Door het hebben van de twee rollen kan het proces niet 'in-control' zijn en kan er niet gesteund worden op het proces van uitgeven van de bevoegdheden.

7.2 Het verstrekken van bevoegdheden voor medewerkers van de eigen afdeling

Er is gebleken dat meeste leidinggevenden niet beschikken over een uitgangspunt voor het gewenste resultaat. In de theorie in H4.1, H4.5.2 en H4.5.3 staat vermeld dat controle als randvoorwaarde noodzakelijk is om 'in-control' te kunnen zijn. Afdelingen die niet 'in-control' van de bevoegdhedenprocessen zijn, kunnen niet steunen op een integere gegevensverwerking in de geautomatiseerde systemen. Samenvattend, afdelingen kunnen niet garanderen dat alleen de juiste medewerkers toegang hebben tot alleen de juiste applicaties. Doordat niet gesteund kan worden op een integere gegevensverwerking in de geautomatiseerde systemen, kan gesteld worden dat er sprake is van een onbetrouwbare informatiebeveiliging en een onbetrouwbare informatievoorziening. Dit in relatie brengend met de doelstelling van dit onderzoek moet vastgesteld worden dat de waarborging van de privacy van de patiënt (patiëntveiligheid) in het geding is.

De oorzaak hiervan is dat het organiseren van activiteiten steeds plaatst vindt in een specifieke situatie. Er is daarom niet een beste manier van organiseren. In alle situaties moet gezocht worden naar een situatie- gebonden oplossing. Structurering heeft betrekking op het probleem van het ontwerpen van een organisatiestructuur waarbinnen mensen en middelen worden afgestemd op de te bereiken doelstelling in een organisatie.

In H4.5.3 en H4.5.4 wordt in de theorie vermeld hoe een organisatie haar organisatie kan structureren. Op dit moment bepaalt een afdeling naar eigen inzicht wie de tekenbevoegde wordt en hoeveel tekenbevoegden zij willen hebben. Ditzelfde geldt voor het uitgeven van de bevoegdheden. Het bevoegdhedenproces verschilt per afdeling. Daarnaast laat de rode draad wel duidelijk zien dat de tekenbevoegden direct, dan wel indirect via een geaccordeerde lijst, handelen in opdracht van hun leidinggevende. Het mag hierbij duidelijk worden dat de 'Soll'-positie grotendeels afhankelijk is van de aard van de werkzaamheden binnen een afdeling. Afdelingen waar de functies en het aanvraag-autorisatieproces worden gestandaardiseerd hebben de uniformiteit als 'Soll'-positie voor de bevoegdheden. H4.6.9.

Belangrijk risico bij het aanvragen van bevoegdheden is het feit dat er rechtstreeks contact mogelijk is tussen de tekenbevoegde en de functioneel beheerder van een systeem. Dit valt te constateren doordat de functioneel beheerder een aanvraag rechtstreeks terugkoppelt aan de tekenbevoegde. Hierbij komt dat de medewerkers van afdeling ICT en bureau FGB geen registratie bijhouden van de verstrekte bevoegdheden. Dit omdat zij niet aansprakelijk zijn voor de

aangevraagde bevoegdheden en omdat de aanvragen die via IDS/ISS binnenkomen terug te vinden zijn in het gebruikersaccount in Clientèle. Het risico dat dreigt is dat de registratie van de bevoegdhedenprocessen omzeild kan worden door aanvragen mondeling in te dienen. Dit blijkt ook voor te komen, refererend aan de onderliggende interviews. Zo kan de 'Soll'-positie niet bereikt worden. Doordat er niet gesteund kan worden op een integere gegevensverwerking in de geautomatiseerde systemen, kan gesteld worden dat er sprake is van een onbetrouwbare informatiebeveiliging en van een onbetrouwbare informatievoorziening. Wanneer dit in relatie gebracht wordt met de doelstelling van dit onderzoek moet worden vastgesteld dat de waarborging van de privacy van de patiënt (de patiëntveiligheid) in het geding is.

7.3 Het verstrekken van bevoegdheden voor medewerkers buiten de eigen afdeling

Er zijn geen dusdanige risico's en problemen gevonden die van significante waarden zijn m.b.t. de doelstelling van dit onderzoek.

7.4 Het uitbreiden/muteren van bevoegdheden

Er zijn geen dusdanige risico's en problemen gevonden die van significante waarden zijn m.b.t. de doelstelling van dit onderzoek.

7.5 Het intrekken van bevoegden als een medewerker extern vertrekt

Bij het opstellen van de huidige situatie is gebleken dat er **nooit controle** op de verstrekte bevoegdheden wordt uitgeoefend. In H4 is aan bod gekomen dat het van belang is om controle uit te oefenen om 'in-control' te zijn, dan wel hoe een bedrijf 'in-control' kan komen. 'In-control' zijn van de bedrijfsprocessen is van het grootste belang voor het functioneren van een organisatie. Het is namelijk pas mogelijk om als organisatie in te spelen op de (te verwachten) ontwikkelingen in de samenleving wanneer de interne processen worden beheerst.

Het hebben van **geen controle** op de uitgegeven bevoegdheden kan gezien worden als het **kernprobleem**. In H6.7 wordt hier dieper op ingegaan.

7.6 Het intrekken van bevoegdheden als een medewerker intern vertrekt

Er zijn geen dusdanige risico's en problemen gevonden die van significante waarden zijn m.b.t. de doelstelling van dit onderzoek.

7.7 Periodieke controle op de verstrekte bevoegdheden

Het is in H7.5 al duidelijk geworden dat er geen controle op uitgegeven bevoegdheden plaatsvindt. Het **waarom** is nog niet bekend. Vooraf zou het antwoord op deze vraag kunnen zijn, dat de leidinggevenden op de interne accountantsdienst vertrouwen. Dit is alleen niet aannemelijk omdat uit de interviews is gebleken dat de interne accountantsdienst alleen de bevoegdheden in de systemen en op papier controleert als onderdeel van de procescontrole. Dit alleen in de onderdelen salarissen, voorraden, inkopen, bouw, apotheek en een deel van de omzet in het kader van DBC's. Hierdoor wordt lang niet iedere afdeling en applicatie van de bevoegdheden gecontroleerd.

Tevens blijkt uit de interviews dat de interne accountantsdienst ook rapporteert aan het hoofd van de gecontroleerde afdeling. Een leidinggevende zou daarom moeten weten of de bevoegdheden van een afdeling (deels) onder de controle van de interne accountantsdienst vallen of niet. Hierbij nog steeds geen antwoord op de waarom-vraag.

De onderliggende interviews wijzen uit dat leidinggevenden geen controle op hun tekenbevoegden uitoefenen, omdat ze geen valide uitgangspunt hebben waarmee ze hun controle kunnen uitvoeren. De hiërarchische leidinggevende houdt geen documentatie bij van de verstrekte bevoegdheden. De leidinggevende beschikt dus niet over een uitgangspunt voor het gewenste resultaat. Refererend naar de theorie in H4.5.2 die hierover spreekt.

Echter, dit geldt niet voor alle afdelingen. Sommige afdelingen verstrekken bevoegdheden op basis van functie en aan de hand van een lijst van nieuwe medewerkers, aldus H6.2.2. Bij deze afdelingen is de 'Soll'-positie wel bekend. De 'Soll'-positie bestaat namelijk uit de bevoegdheden die bij een bepaalde functie horen. Echter, op deze afdelingen vindt geen controle op de verstrekte bevoegdheden plaats. Onderliggende interviews wijzen uit dat controle onbegonnen werk is, door de grote hoeveelheid medewerkers en de bedrijfsdrukte op een afdeling.

Het is duidelijk geworden wat de problemen zijn en in welk proces de problemen zitten. In het volgende hoofdstuk volgt de gewenste situatie.

8 De gewenste situatie

Na de beschrijving van de huidige situatie in H5 en de probleem-analyse in H6 wordt nu de gewenste situatie weergegeven waarna de aanbeveling volgt. Hierbij worde de aanpassing t.o.v. de huidige situatie in een oranje vlak weergegeven. Waarom de aanbeveling geldt wordt aan de hand van de theorie in H4 besproken.

8.1 De tekenbevoegde

Het bevoegdhedenproces begint met het aanstellen van een tekenbevoegde. Een afdeling bepaalt naar eigen inzicht hoeveel medewerkers de taak tekenbevoegden naast hun eigen functie krijgen. Hierbij maken de medewerkers zelf de keuze of zij tekenbevoegde willen zijn.

8.1.1 Het proces

1) De hiërarchisch leidinggevende zoekt een medewerker die het in zich heeft om als tekenbevoegde te fungeren.
2) De hiërarchisch leidinggevende mandateert de medewerker en de medewerker tekent de mandatering eveneens.
3) De mandatering wordt via de interne post naar ICT bevoegdhedenbeer opgestuurd.
4) ICT bevoegdhedenbeheer controleert de mandatering op juistheid en volledigheid.
5) Na de controle van ICT bevoegdhedenbeheer zijn er meerdere mogelijkheden voor de vervolg actie:
    a) Een afgekeurde mandatering gaat, met motivatie, retour naar de afzender
    b) Op de goedgekeurde mandatering staat vermeld dat de oude tekenbevoegde moet worden verwijderd. Deze handeling wordt eerst uitgevoerd voordat de mandatering wordt uitgevoerd.
    c) De mandatering wordt uitgevoerd.
6) ICT bevoegdhedenbeheer documenteert de mandatering in ringbandmappen en scant deze (in de loop van de tijd) in. Tevens houden zij een eigen registratie in Excel bij.
7) De medewerker is tekenbevoegd.

De tekenbevoegde kan nu bevoegdheden aanvragen via IDS/ISS voor de medewerkers. De tekenbevoegden hebben als enigen toegang tot deze systemen

Voor processchema zie figuur 12 in de bijlage.

8.1.2 Waarom deze aanbeveling?

Op iedere afdeling in het ziekenhuis is het mogelijk dat de hiërarchisch leidinggevende zichzelf mandateert. Het wordt aanbevolen dat een hiërarchisch leidinggevende alleen een ondergeschikte mandateert als tekenbevoegde. Echter, in H3 werd aangegeven dat het niet in iedere situatie geldt. Het toepassen van contole-technische functiescheiding bij de structurering van organisaties dient op rationele gronden plaats te vinden, aldus H4.5.3. Daarnaast dient men per afdeling na te gaan of het volgens de theorie van H4.6.6 technisch, operationeel en economisch haalbaar is.

Het maken van uitzonderingen in de organisatie is dus mogelijk. Maar op basis van de huidige situatie, dat op iedere afdeling de hiërarchisch leidinggevende ook als tekenbevoegde kan fungeren, is dit onacceptabel als het gaat om een betrouwbare informatiebeveiliging en een betrouwbare informatievoorziening.

8.2 Het verstrekken van bevoegdheden voor medewerkers van de eigen afdeling

Het verstrekken van bevoegdheden voor medewerker van de eigen afdelingen was in de huidige situatie onderverdeeld in drie mogelijkheden:

- Financiële afdeling
- Verpleegafdeling
- Beheerafdeling

Aan het eind van ieder proces volgt het algemeen vervolg dat staat weergegeven in H6.2.4 waarvan het proces niet wordt veranderd.

8.2.1 Financiële afdeling

Dat een medewerker constateert dat deze te weinig bevoegdheden heeft om zijn functie uit te voeren zal in de gewenste situatie niet voorkomen. Het aanvraag proces zal geschieden volgens de methodiek van de verpleegafdeling dan wel de beheerafdeling.

8.2.2 Verpleegafdeling

1) Periodiek ontvangt de tekenbevoegde de lijst met nieuwe medewerkers van afdeling Personeels-zaken.
2) De tekenbevoegde vraagt, op basis van de functie die vermeld staat op de ontvangen lijst, de bevoegdheden tijdig aan via IDS/ISS.

Dit proces kan worden weergegeven als functiestandaardisatie.

8.2.3 Beheerafdeling

1) Een nieuwe medewerker op de afdeling.
2) De hiërarchische leidinggevende van de afdeling geeft opdracht aan de tekenbevoegde om bevoegdheden aan te vragen voor de nieuwe medewerker.
3) De hiërarchisch leidinggevende van de afdeling registreert de aanvraag die hij doorstuurt naar de tekenbevoegde.

Bij dit proces worden bevoegdheden individueel verstrekt, waardoor het wordt beoordeeld als niet-standaardisatie.

Het algemeen vervolg was correct opgesteld, zie H6.2.4. Voor processchema zie figuur 13 en 14 in de bijlage.

8.2.4 Waarom deze aanbeveling?

Aan de hand van de 'Soll'-positie kan de leidinggevende, of ondergeschikte in opdracht van de leidinggevende (geen tekenbevoegde), de bevoegdheden in de systemen controleren (de 'Ist'-positie).

Terugkijkend op H7.2 kan worden geconcludeerd dat de huidige 'Soll'-positie niet kan worden vastgesteld. Stellig wordt dan ook aanbevolen dat de leidinggevende voorzien wordt van een 'Soll'-positie. In H4.6.9 wordt uitleg gegeven over standaardisatie en in welke vormen het mogelijk is. De leidinggevende kan bevoegdheden standaardiseren door aansluiting te vinden bij een uniformiteit binnen de afdeling, of de leidinggevende kan bevoegdheden niet standaardiseren en op individueel niveau bepalen wie welke bevoegdheden mag hebben.

Wanneer er op een afdeling veel werknemers zijn die dezelfde functie uitoefenen kan gedacht worden om het geheel te standaardiseren; op enkele verpleegafdelingen wordt al aan standaardisatie van bevoegdheden naar aanleiding van de functie gedaan.

Wanneer bij het aanvragen van bevoegdheden veel maatwerk komt kijken, zoals op de afdeling van bureau FGB, is algehele standaardisatie niet haalbaar, kijkende naar de operationele haalbaarheid van H4.6.6.

Afdelingen moeten individueel bepalen in welk 'straatje' zij vallen. Is dat waar veel dezelfde functies uitgeoefend worden en waar standaardisatie van zeer grote invloed kan zijn, of verricht de afdeling dusdanige aanvragen die voor geen een medewerker gelijk is, dat zij niet voor standaardisatie kiest maar voor de handmatige aanvraag. De verantwoordelijkheid hiervan ligt bij de hiërarchische leidinggevende. Dit persoon moet ervoor zorgen dat de afdeling 'in-control' komt en hierbij moet zij kijken naar welke keuze het best is voor de afdeling. Refererend naar H4.5.3 die betrekking hebben op de organisatie om 'in-control' te komen.

Wanneer een afdeling voor standaardisatie kiest kan dit overigens niet voor 100% gebeuren. Het proces 'het verstrekken van bevoegdheden voor medewerkers buiten de eigen afdeling', blijft maatwerk.

8.3 Het verstrekken van bevoegdheden voor medewerkers buiten de eigen afdeling

Het proces dat is beschreven in H6.3 voldoet al aan de gewenste situatie daar er in H7 geen problemen zijn gevonden. Daarom wordt dit niet herhaald.

8.4 Het uitbreiden/muteren van bevoegdheden

Het proces dat is beschreven in H6.4 voldoet al aan de gewenste situatie daar er in H7 geen problemen zijn gevonden. Daarom wordt dit niet herhaald.

8.5 Het intrekken van bevoegdheden als een medewerker extern vertrekt

Bij het intrekken van bevoegdheden als een medewerker extern vertrekt zijn er twee zaken die moeten worden verwijderd: het gebruikers account en de bevoegdheden. Eerst wordt het proces besproken over verwijderen van accounts, daarna het verwijderen van bevoegdheden.

8.5.1 Het verwijderen van gebruikers accounts

1) Een medewerker vertrekt extern.
2) Een medewerker van personeelszaken controleert of de vertrekkend medewerker een Peoplesoft account heeft.
    a) De vertrekkend medewerker beschikt niet over Peolplesoft account.
    b) De vertrekkend medewerker beschikt over een Peoplesoft account en een micro-sectienummer.
    c) De vertrekkend medewerker beschikt over een Peoplesoft account, maar geen micro-sectienummer.

Iedere persoon die voor het UMCG werkt heeft een ZIS-account nodig om de functie uit te kunnen voeren. Dit kunnen interne medewerkers dan wel externe medewerkers zijn. Interne medewerkers staan op de loonlijst van het UMCG en daardoor komen zij ook in het Peoplesoft systeem. Met het Peoplesoft systeem is het mogelijk om een koppeling te maken met het ZIS systeem. Externe medewerkers ontvangen geen loon van het UMCG en staan daardoor niet in het Peoplesoft systeem. De externe medewerker heeft daardoor ook geen Peoplesoft account.

Geen account

3) De medewerker van personeelszaken koppelt een einddatum aan het ZIS-account van de vertrekkend medewerker.
4) ICT bevoegdheden koppelt een vervaldatum aan het ZIS-account van de medewerker.
5) Het ZIS controleert tijdens het inloggen op de ontslagdatum of vervaldatum en geeft dertig dagen voor de einddatum een melding.
6) Inloggen blijft tot achtenveertig dagen na einddatum mogelijk, de melding voor vervaldatum wordt continu weer gegeven. Na achtenzeventig dagen de melding te hebben gehad, wordt het account definitief verwijderd. Dit gebeurt automatisch door het systeem. Hierna is het gebruikersaccount verwijderd.

Wel een account en een microsectienummer

3) De medewerker van personeelszaken koppelt de ontslagdatum aan het Peoplesoft account.
4) De medewerker die in Peoplesoft geregistreerd staat heeft een personeelsnummer. Dit nummer is via een elementnummer gekoppeld aan een microsectienummer in het ZIS, waardoor de einddatum ook in het ZIS-account wordt ingevuld. Hierbij is dit proces beëindigd.

Wel een account maar geen microsectienummer

3) De medewerker van personeelszaken koppelt de ontslagdatum aan het Peoplesoft account.
4) ICT bevoegdheden beheer kan via een toegestane workaround een medewerker toegang geven tot het ZIS. Zij koppelt het microsectienummer aan het personeelsnummer van de vertrekkend medewerker en voegt de medewerker toe in BEVPER. Deze gebruiker heet in het ZIS 'toekomstige ZIS gebruiker'.

Wanneer de medewerker nog niet is verwijderd bestaat er de kans op de volgende procedure.

5) Het microsectienummer van een medewerker wordt later alsnog bekend. ICT bevoegdhedenbeheer zorgt via een batch voor de koppeling tussen naam en usernummer.

Deze procedure zal in de toekomst automatisch worden gesynchroniseerd.
Het kan voorkomen dat dit proces niet wordt gestart, terwijl de medewerker niet meer werkzaam is in het UMCG. Hiervoor heeft het UMCG een script dat automatisch controleert op niet-gebruikte gebruikeraccounts in het AD. De procedure voor de AD loopt als volgt:

1) Wanneer een account langer dan een half jaar niet wordt gebruikt wordt het account geblokkeerd in de OU.

2) Wanneer het account in de OU komt heeft deze 30 dagen om weer actief te worden. Dit kan d.m.v. een helpdesk call. De volgende procedures kunnen volgen:
   a) Het account staat langer dan dertig dagen in de OU. Hierdoor wordt het account automatisch verwijderd.
   b) Het account staat minder dan dertig dagen in de OU.

Vervolg op 2)b.

3) De mogelijkheid is nog aanwezig om het account te activeren. Dit hangt af van het feit of er een helpdesk call komt.
   a) De call komt niet, er worden geen handelingen verder uitgevoerd.
   b) De call komt, het account wordt geheractiveerd en teruggeplaatst naar de medewerker.

Behalve dat het account van de vertrekkende medewerker moet worden verwijderd, moeten ook alle bevoegdheden van de medewerker worden verwijderd.

Aan het eind van dit proces moet er een periodieke controle komen. Deze controle is omschreven in H8.7.

8.5.2 Verwijderen van bevoegdheden

1) Een medewerker vertrekt extern.
2) De hiërarchisch leidinggevende denkt niet vanzelfsprekend aan het intrekken van bevoegdheden als een medewerker vertrekt. Hierdoor bestaat in de procedure een tweedeling.
   a) De hiërarchische leidinggevende meldt het vertrek niet aan de tekenbevoegde waardoor de bevoegdheden in het systeem blijven bestaan en het proces staakt. In H. 7.5.1 wordt gemeld welke actie het AD dan neemt.
   b) De hiërarchische leidinggevende meldt het vertrek aan de tekenbevoegde.
3) De tekenbevoegde verwijdert de bevoegdheden van de medewerker.

Voor processchema zie figuur 18 in de bijlage.

Aan het eind van dit proces moet er een periodieke controle komen. Deze controle is omschreven in H8.7.

8.6 Het intrekken van bevoegdheden als een medewerker intern vertrekt

Het proces dat is beschreven in H6.6 voldoet al aan de gewenste situatie daar er in H7 geen problemen zijn gevonden. Daarom wordt dit niet herhaald.

8.7 Periodieke controle op de verstrekte bevoegdheden

Voor het controleren van de bevoegdheden is het noodzakelijk dat er een 'Soll'-positie aanwezig is. Vanaf hier start het proces.

8.7.1 Het proces

1) 'Soll'-positie
   a. Beschikbaar.
   b. Niet beschikbaar.

Ad 1)b. het opstellen van een 'Soll'-positie.

2) 'Soll'-positie wordt vergelijken met de 'Ist'-positie door een medewerker van de afdeling (behalve de tekenbevoegde).
3) Constateren van afwijkingen in de 'Ist'-positie m.b.t. de 'Soll'-positie.
   a. Nee
   b. Ja

Vervolg 3)a.

4) Controle rapporteren aan leidinggevende waarna het proces stopt.

Vervolg 3)b.

4) Het analyseren van de afwijkingen en het beoordelen van de afwijkingen.
5) De afwijkingen bespreken met de tekenbevoegde van de afdeling.
6) Beoordelen of de afwijking akkoord is.
   a) Afwijking is akkoord.
   b) Afwijking is niet akkoord.

Vervolg 6)a.

7) Controle rapporteren aan leidinggevende waarna het proces stopt.

Vervolg 6)b.
7) De afwijking wordt aangepast.
8) De afwijking wordt geëvalueerd waarna het gerapporteerd wordt aan de leidinggevende en waarna het proces stopt.

Voor processchema zie figuur 22 in de bijlage.

8.7.2 Waarom deze aanbeveling?

Daar de verantwoordelijkheid van de uitgegeven bevoegdheden bij de leidinggevende ligt, wordt dringend aanbevolen dat leidinggevenden hun verantwoordelijkheid nemen en controle op de bevoegdhedenprocessen uitoefenen. Momenteel zijn de meeste afdelingen hier niet toe in staat, omdat zij niet beschikken over een 'Soll'-positie. De afdelingen die momenteel wel over een 'Soll'-positie beschikken moeten zorgen dat ze 'in-control' van de bevoegdhedenprocessen komen.

Zodra leidinggevenden over een 'Soll'-positie beschikken hebben zij de middelen om controle uit te kunnen oefenen. Leidinggevenden hebben rechtstreeks of via hun tekenbevoegde toegang tot de 'Ist'-positie in Clientèle en Vegasuit (aanvraag voor 18 mei 2011).

De 'Ist'-positie kan de leidinggevende, of een ondergeschikte in opdracht van de leidinggevende (geen tekenbevoegde), vervolgens vergelijken met de 'Soll'-positie. Het resultaat van hun controleactiviteiten bestaat uit het signaleren of er ergens tekortkomingen zijn. Met het constateren of er afwijkingen zijn tussen het bereikte resultaat en de doelstelling (de 'Soll'-positie) mag echter niet worden volstaan. De gevonden afwijkingen moeten namelijk worden geanalyseerd en beoordeeld. Ook moeten ze met de tekenbevoegden worden besproken.

Bespreking van de gevonden afwijkingen met de tekenbevoegde verhoogt het bewustzijn van de tekenbevoegde. Uit analyse zal moeten blijken wat de oorzaken zijn geweest die tot de geconstateerde afwijkingen hebben geleid. Op grond van deze kennis kunnen maatregelen worden getroffen om in de toekomst soortgelijke afwijkingen te voorkomen.

Uiteraard zal in een later stadium moeten worden nagegaan in hoeverre deze correctieve maatregelen effect hebben gehad; de evaluatie. Afwijkingen tussen het bereikte en het gewenste resultaat behoeven niet altijd het gevolg te zijn van een onjuiste of minder juiste (wijze van) uitvoering; ook het gestelde doel –de 'Soll'-positie – kan in de gegeven omstandigheden niet reëel zijn.

Wanneer het verwezenlijken van een doelstelling onrealistisch is of door omstandigheden onhaalbaar is geworden, zal de doelstelling moeten worden 'bijgesteld'.

In het volgende hoofdstuk wordt het implementatietraject aangegeven.

9 De implementatie

In H6 werd de huidige situatie beschreven en in H8 de gewenste situatie. Om het verschil tussen de huidige situatie en de gewenste situatie te overbruggen, wordt in dit hoofdstuk een stappenplan aan de hand gedaan. Door het stappenplan te volgen wordt geleidelijk de gewenste situatie bereikt.

Een implementatietraject behoort tot de scope van dit onderzoek. Een implementatietraject, zoals gebruikelijk is bij meer technisch gerichte opleidingen, maakt geen onderdeel uit van de opleiding Accountancy. Derhalve wordt in de vorm van een stappenplan een voorzet voor een implementatietraject gegeven.

In het stappenplan wordt onderscheid gemaakt tussen het stappenplan van een afdeling die standaardiseert en een afdeling die dat niet doet.

9.1 Standaardisatie

In deze paragraaf wordt het implementatietraject voor standaardisatie behandeld.

9.1.1 CTFS creëren

Een succesvolle implementatie is afhankelijk van de randvoorwaarden. De randvoorwaarden om een succes te behalen staan vermeld in H4.8. In H8.1.1 wordt aanbevolen dat een hiërarchisch leidinggevende altijd een ander mandateert dan zichzelf. Het is daarom zaak het beheer op tekenbevoegden op efficiënte en effectieve wijze te organiseren. ICT bevoegdhedenbeheer is hier bij uitstek de juiste kandidaat voor. Om een succesvolle implementatie te bewerkstellingen, dient ICT bevoegdhedenbeheer met terugwerkende kracht alle tekenbevoegden te controleren op een hiërarchische leidinggevende functie. Dit kan eenvoudig via de norm en standenlijst van de meest recente peildatum. Tekenbevoegd zijn met een hiërarchische leidinggevende functie is echter wel mogelijk. Zie hiervoor naar H8.1.2.

9.1.2 'Soll'-positie bepalen

De tweede stap is het komen tot een grondslag voor een 'Soll'-positie voor alle afdelingen. Wanneer een afdeling al een duidelijke 'Soll'-positie heeft kan zij deze stap overslaan. Afdelingen die nog geen duidelijke 'Soll'-positie hebben, moeten een 'Soll'-positie creëren.

9.1.3 Uniformiteit bepalen

De keuze is gemaakt voor standaardisatie, dit betekent dat de afdeling naar een uniformiteit binnen de afdeling moet zoeken. Hierbij kan gedacht worden aan de functies van medewerkers. De functie wordt ook als voorbeeld gebruikt in het vervolg van het implementatietraject.

9.1.4 Opstellen

Nadat bekend is wat de uniformiteit binnen de afdeling is, is het zaak om een lijst van standaardbevoegdheden per functie op te stellen. Dit proces kan het best breed over de afdeling getrokken worden en niet gelimiteerd worden tot een select gezelschap. Dit zorgt voor een juistere en meer volledige lijst van bevoegdheden die bij een functie noodzakelijk zijn. Het opstellen van standaardbevoegdheden is, gezien het aantal applicaties, veel werk en de medewerkers op de werkvloer worden uiteindelijk in hun vrijheden ingeperkt. Dit tot het succesvol brengen van de implementatie, refererend naar H4.8.

9.1.5 Verankeren

Wanneer er een definitieve lijst met standaardbevoegdheden opgesteld is, verankert de hiërarchische leidinggevende de standaardbevoegdheden met een handtekening.

9.1.6 Lijst van medewerkers

Wanneer de lijst met standaardbevoegdheden is opgesteld, is het tijd op bij de afdeling personeelszaken van de sector een lijst van medewerkers van de afdeling op te vragen.

Hierop moet staan vermeld:
- De volledige naam
- De functie
- Het personeelsnummer

De volledige naam vergemakkelijkt de communicatie, de functie is het aanknopingspunt voor de bevoegdhedenprocessen en het personeelsnummer kan gevraagd worden tijdens het verstrekken van bevoegdheden.

9.1.7 Afspraken

De afdeling moet met de personeelszaken van de afdeling duidelijke afspraken maken over het periodiek aanleveren van een lijst met de mutatie van medewerkers. Bevoegdheden worden op functie verstrekt, verandert de functie of komt iemand nieuw in een functie dan moet dat tijdig bekend zijn in verband met het aanvragen, muteren en verwijderen van bevoegdheden.

9.1.8 Analyse

Nu bekend is wie welke bevoegdheden mag hebben, begint de grootste stap. De tekenbevoegde van de afdeling verwerkt, volgens de lijst van de afdeling personeelszaken, alle medewerkers één voor één. Per medewerker controleert de tekenbevoegde welke bevoegdheden er uitgegeven zijn en welke bevoegdheden er bij de functie van die medewerker horen. Van de geconstateerde afwijkingen maakt de tekenbevoegde correcties. De looptijd van dit proces varieert.

Dit is afhankelijk van:
- Het aantal tekenbevoegden
- Het aantal applicaties
- Het aantal medewerkers

Het is mogelijk om dit proces te versnellen door tijdelijk meer tekenbevoegden aan te stellen.

9.1.9 Controle

Nadat de analyse is afgerond oefent de hiërarchische leidinggevende (of een ondergeschikte behalve de tekenbevoegde) controle uit op de uitgegeven bevoegdheden. Wanneer er afwijkingen worden geconstateerd, worden de afwijkingen besproken met de tekenbevoegde. Worden er geen afwijkingen geconstateerd dan is de 'Soll'-positie bereikt.

9.1.10 Rapportagestandaard

Met het bereiken van de 'Soll'-positie is de implementatie nog niet afgerond. Er zullen in de toekomst mutaties in de bevoegdheden plaatsvinden en het personeel zal verlopen. Daarom is het belangrijk om te komen tot een betrouwbare rapportagestandaard. Geen van de afdelingen heeft eerder een integrale controle op de verstrekte bevoegdheden uitgevoerd. De aanknopingspunten ontbraken en om deze reden is het noodzakelijk dat in samenwerking met ICT, gekomen wordt tot een betrouwbare, bruikbare rapportagestandaard. Gebeurt dit niet, dan verzanden leidinggevenden bij de controle, omdat ze niet doelmatig en doelgericht controle uit kunnen oefenen. Door het niet doelmatig en doelgericht kunnen controleren nodigt het uitoefenen van de controle niet uit en dit moet voorkomen worden. De leidinggevende moet een eenvoudige lijst kunnen ontvangen waarop gevinkt kan worden bij de controle. Hierbij is de implementatie voltooid.

9.1.11 Onderhouden

Het is mogelijk dat applicaties in de loop van de tijd veranderen en dat bevoegdheden verschuiven tussen functies. De lijst met standaardbevoegdheden moet daarom periodiek geüpdatet en geaccordeerd worden. Dit is cruciaal omdat in een situatie waarin dit niet gebeurt, er toch doorgewerkt moet worden. Het gevolg is dat bevoegdheden buiten de standaardbevoegdheden verstrekt worden, wat resulteert in niet-standaardisatie zonder registratie.

9.2 Niet-standaardisatie

In deze paragraaf wordt het implementatietraject voor niet-standaardisatie behandeld.

9.2.1 CTFS creëren

Een succesvolle implementatie is afhankelijk van de randvoorwaarden. De randvoorwaarden om een succes te behalen staan vermeld in H4.8. In H8.1.1 wordt aanbevolen dat een hiërarchisch leidinggevende altijd een ander mandateert dan zichzelf. Het is daarom zaak het beheer op tekenbevoegden op efficiënte en effectieve wijze te organiseren. ICT bevoegdhedenbeheer is hier bij uitstek de juiste kandidaat voor. Om een succesvolle implementatie te bewerkstellingen, dient ICT bevoegdhedenbeheer met terugwerkende kracht alle tekenbevoegden te controleren op een hiërarchische leidinggevende functie. Dit kan eenvoudig via de norm en standenlijst van de meest recente

peildatum. Tekenbevoegd zijn met een hiërarchische leidinggevende functie is echter wel mogelijk. Zie hiervoor naar H8.1.2.

9.2.2 'Soll'-positie bepalen

De tweede stap is het komen tot een grondslag voor een 'Soll'-positie voor alle afdelingen. Wanneer een afdeling al een duidelijke 'Soll'-positie heeft kan zij deze stap overslaan. Afdelingen die nog geen duidelijke 'Soll'-positie hebben, moeten een 'Soll'-positie creëren.

9.2.3 Juist en volledig

Wanneer een afdeling de keuze maakt om niet gestandaardiseerd te gaan werken betekent dit dat de hiërarchisch leidinggevende een zo juist en volledig mogelijke registratie moet bijhouden van de verstrekte opdrachten. Opdrachten in het kader van het verstrekken, muteren en verwijderen van bevoegdheden. De registratie moet zo juist en volledig mogelijk zijn omdat het de basis vormt voor de controle. Het vormt de zogenoemde 'Soll'-positie. Daarnaast kan er aan de hand van de registratie op een efficiënte en effectieve manier gecontroleerd worden. Het is zaak om vooraf goed over de manier van registreren na te denken. Een map vol e-mail werkt met het oog op de controle niet efficiënt of effectief. Tip: een registratie in Access met databasefunctionaliteit. Door invoer- en applicatiecontroles kunnen direct de meest voorkomende fouten voorkomen worden.

9.2.4 Invullen en onderhouden

Nu de hiërarchische leidinggevende over een registratie beschikt, is het tijd om deze in te vullen. Van nu af aan registreert de leidinggevende elke opdracht tot het uitgeven, muteren of verwijderen van bevoegdheden. Dit moet refererend naar de voorgaande alinea zo juist en volledig mogelijk. Om de gap met het verleden te sluiten, moet de leidinggevende de uitgegeven bevoegdheden in de registratie opnemen. Gebeurt dit niet, dan heeft een leidinggevende een onbetrouwbare 'Soll'-positie en dient de registratie als schijnveiligheid. Heeft een leidinggevende een up-to-date registratie, dan hoeft in principe geen controle op de verstrekte bevoegdheden uit te voeren, omdat de 'Soll'-positie in dit geval uit de 'Ist'-positie voortkomt.

9.2.5 Rapportagestandaard

Met het bereiken van de 'Soll'-positie is de implementatie nog niet afgerond. Er zullen in de toekomst mutaties in de bevoegdheden plaatsvinden en het personeel zal verlopen. Daarom is het belangrijk om te komen tot een betrouwbare rapportagestandaard. Geen van de afdelingen heeft eerder een integrale controle op de verstrekte bevoegdheden uitgevoerd. De aanknopingspunten ontbraken en om deze reden is het noodzakelijk dat in samenwerking met ICT, gekomen wordt tot een betrouwbare, bruikbare rapportagestandaard. Gebeurt dit niet, dan verzanden leidinggevenden bij de controle, omdat ze niet doelmatig en doelgericht controle uit kunnen oefenen. Door het niet doelmatig en doelgericht kunnen controleren nodigt het uitoefenen van de controle niet uit en dit moet voorkomen worden. De leidinggevende moet een eenvoudige lijst kunnen ontvangen waarop gevinkt kan worden bij de controle. Hierbij is de implementatie voltooid.

9.3 Schematisch

In de twee voorgaande sub-paragrafen is stap voor stap vermeld welke handelingen verricht dienen te worden voor de twee keuze mogelijkheden te weten: standaardisatie dan wel niet-standaardisatie. In figuur 10 worden de stappen onder elkaar gezet om het autorisatieproces duidelijk te maken. In de eerste kolom staat welke handeling verricht moet worden. De twee middelste kolommen laten voor de keuzemogelijkheden zien welke handeling wel of niet van toepassing is. In de laatste kolom is vermeld onder wiens verantwoordelijkheid de handeling valt.

	Standaardiseren	Niet standaardiseren	Verantwoordelijk
Controle-technische functiescheiding creëren bij mandatering	•	•	ICT bevoegdhedenbeheer
Grondslag 'Soll'-positie bepalen	•	•	Hiërarchisch leidinggevende
Uniformiteit bepalen	•		Hiërarchisch leidinggevende
Lijst met standaardbevoegdheden opstellen	•		Afdelingsbreed
Lijst met standaardbevoegdheden verankeren	•		Hiërarchisch leidinggevende
Lijst van medewerkers van de afdeling bij personeelszaken van de sector opvragen	•		Hiërarchisch leidinggevende
Afspraken met personeelszaken maken over periodiek aanleveren lijst met mutatie van medewerkers	•		Hiërarchisch leidinggevende
Analyse 'Ist'-positie en 'Soll'-positie	•		Tekenbevoegde
Controle analyse	•		Hiërarchisch leidinggevende
Bijhouden zo juist en volledig mogelijke registratie		•	Hiërarchisch leidinggevende
Registratie invullen en onderhouden		•	Hiërarchisch leidinggevende
Betrouwbare rapportagestandaard met ICT afspreken	•	•	Hiërarchisch leidinggevende
Lijst met standaardbevoegdheden onderhouden	•		Hiërarchisch leidinggevende

Figuur 9 Stappenplan

10 Conclusies

De doelstelling van dit onderzoek is het geven van een advies aan de afdelingen FGB/ICT van het UMCG omtrent een patiëntvriendelijke[35], patiëntveilige[36], efficiënte inrichting van de procedures voor het uitgeven, intrekken en muteren van bevoegdheden bij het gebruik van UMCG-brede applicaties ten einde:

- Duidelijkheid te scheppen voor het huidige personeel;
- Efficiënter het proces te laten verlopen;
- Een UMCG-brede standaardisatie te creëren als het gaat om autorisaties;
- Een meer betrouwbare informatiebeveiliging en informatievoorziening te creëren.

Bureau FGB heeft daarbij gefungeerd als primaire opdrachtgever.

Op aanwijzingen van de opdrachtgever, heeft onze aandacht van meet af aan bij de patiëntveiligheid gelegen.

De subvragen bij dit onderzoek zijn:
1) Wat leert de theorie ons over het toevoegen, muteren en verwijderen van autorisaties?
2) Hoe ziet het (relevante) bedrijfsprofiel van het UMCG eruit?
3) Hoe ziet de huidige situatie omtrent het toevoegen, muteren en verwijderen van autorisaties eruit?
4) Welke knelpunten doen zich voor in de huidige situatie?
5) Waarom zijn dit knelpunten?
6) Hoe kunnen deze knelpunten, volgens de theorie, verholpen worden?
7) Welke oplossing heeft de voorkeur?
8) Hoe ziet de gewenste situatie omtrent het toevoegen, muteren en verwijderen van autorisaties eruit?
9) Hoe kan de gewenste situatie bereikt worden? Welke conclusies kunnen worden getrokken?
10) Welke aanbevelingen kunnen worden gedaan?

Aan sommige subvragen kunnen nu conclusies worden verbonden:
1) Autorisaties vallen onder de organisatorische beveiliging. Hierbij is het vooral van belang dat er bij autorisaties scheiding wordt gemaakt tussen de beschikkende, registrerende en uitvoerende functie.
2) N.v.t. voor een conclusie.
3) N.v.t. voor een conclusie.
4) Knelpunten zijn; dat er niet op iedere afdeling sprake is van een controle-technische functiescheiding (CTFS) en het niet 'in-control' zijn van de procedure m.b.t. het aanvragen, muteren en verwijderen van bevoegdheden.
5) Dit zijn knelpunten omdat er niet gebouwd kan worden op een betrouwbare informatievoorziening en informatiebeveiliging.
6) Deze kunnen worden verholpen door een 'Soll'-positie te realiseren waarna controle op de uitgegeven bevoegdheden wordt uitgevoerd.
7) Meerdere conclusies zijn getrokken:
   a. CTFS op iedere afdeling, hiërarchische leidinggevende mag zichzelf niet mandateren.
   b. Afdeling specifiek bepalen hoe het autorisatieproces wordt opgesteld, standaardisatie dan wel niet-standaardisatie.
   c. Controle uitoefenen op de uitgegeven autorisaties.
8) N.v.t. voor een conclusie.
9) N.v.t. voor een conclusie.
10) N.v.t. voor een conclusie.
11) Zie volgende hoofdstuk.

[35] Patiëntvriendelijkheid wordt hier gedefinieerd als de vertraging die de patiënt ondervindt door de procedure
[36] Patiëntveiligheid wordt hier gedefinieerd als de waarborging van de privacy van de patiënt

11 Aanbevelingen

Nu de conclusies zijn gegeven op de subvragen die leiden tot de kern van het onderzoek worden er nu aanbevelingen gegeven tot deze relevante subvragen. De subvragen staan vermeld in H10.

1) N.v.t. voor een aanbeveling.
2) N.v.t. voor een aanbeveling.
3) N.v.t. voor een aanbeveling.
4) N.v.t. voor een aanbeveling.
5) N.v.t. voor een aanbeveling.
6)
    a. Het afdwingen van controle-technische functiescheiding bij de mandatering van medewerkers. Dit door belangen tegenstelling te creëren en ongewenste functiecombinaties tegen te gaan.
    b. Daarnaast moet er een 'Soll'-positie worden gecreëerd voor de bevoegdhedenprocessen. Volgens de theorie kan dit via standaardisatie dan wel niet-standaardisatie.
    c. Het uitoefenen van controles op de uitgegeven bevoegdheden door de hiërarchische leidinggevende dan wel een medewerker van de afdeling, dit mag dan niet de tekenbevoegde zijn.
7)
    a. De belangrijkste aanbeveling hierbij is dat de hiërarchische leidinggevende zichzelf niet mag mandateren waardoor deze niet meer de beschikkende en registrerende functie heeft. Meer hierover staat vermeld in H8.1.
    b. De aanbeveling bij het creëren van de 'Soll'-positie luidt, hiërarchische leidinggevenden moeten de verantwoordelijkheid nemen tot het maken van een keuze, standaardisatie dan wel niet-standaardisatie. Deze keuze kunnen zij o.a. maken op basis van wat er staat vermeld in H8.2.
    c. Het is noodzakelijk om controle uit te voeren op de uitgegeven bevoegdheden om 'in-control' te zijn. Het proces m.b.t. de autorisaties blijft hierdoor up-to-date en 'schoon'. Meer over deze aanbeveling staat vermeld in H8.7.
8) N.v.t. voor een aanbeveling.
9) N.v.t. voor een aanbeveling.
10) N.v.t. voor een aanbeveling.
11) N.v.t. voor een aanbeveling.

Uit de aanbevelingen blijkt duidelijk dat de patiëntveiligheid in de huidige situatie in het geding is. Daarnaast is vastgesteld dat afdelingen niet 'in-control' zijn van de bevoegdhedenprocessen.

Wanneer de inhoud van dit adviesrapport in relatie wordt gebracht met de doelstelling, kan geconcludeerd worden dat de doelstelling is behaald:

- Door de procedure te documenteren is er duidelijkheid geschapen voor het huidige personeel.
- Door de controlefunctie in te voeren worden bevoegdheden meer up-to-date gehouden.
- Dankzij de controlefunctie blijven bevoegdheden niet langer tot in lengte van dagen in de applicaties staan. Bepaalde bevoegdhedenprocessen, zoals het verwijderen van bevoegdheden, verlopen hierdoor efficiënter. Ook neemt de patiëntveiligheid hierdoor toe.
- Door het creëren van een 'Soll'-positie voor de bevoegdhedenprocessen wordt standaardisatie gecreëerd op afdelingsniveau. Standaardisatie op organisatieniveau wordt in het voorgaande hoofdstuk duidelijk afgeraden.
- Door de controlefunctie toe te passen wordt er een meer betrouwbare informatiebeveiliging en meer betrouwbare informatievoorziening gecreëerd.
- Ondanks dat er wijzigingen in het verloop van de bevoegdhedenprocessen zijn aangebracht, blijft de **patiëntvriendelijkheid** gewaarborgd.

BIBLIOGRAFIE

De bronvermelding wordt onderscheiden in websites, literatuur en rapporten.

WEBSITES

IBpedia. (n.d.). Retrieved juni 2, 2011, from IBpedia: http://ibpedia.nl/images/5/5c/Dreigingen_-_Creative_Commons.png

IBpedia. (n.d.). Retrieved juli 2, 2011, from IBpedia: http://ibpedia.nl/images/5/5c/Dreigingen_-_Creative_Commons.png

Info over beveiligingskubus. (n.d.). Retrieved juli 3, 2011, from Beveiligingskubus: http://www.informatie.nl/images/9/9711p25.gif

Info over ketens. (n.d.). Retrieved mei 2011, from Ketens & netwerken: http://www.ketens-netwerken.nl/begrippen#do

Info over Organizational Unit. (n.d.). Retrieved mei 2011, from Organizational Unit: http://i.technet.microsoft.com/cc758565.b0ba9974-c238-42e5-b96c-dcb7deffe84c*en-us,WS.10).gif

Info over Organizational Unit. (n.d.). Retrieved mei 2011, from Microsoft: http://technet.microsoft.com/en-us/libary/cc758565%28ws.10%29.aspx

Info over PeopleSoft. (n.d.). Retrieved mei 2011, from PeopleSoft: http:intranet.od.umcg.nl/fgb/fgb/detail.asp?id=4

Instruct online. (n.d.). Retrieved juli 2, 2011, from Instruct online: http://www.instruct-online.nl/_inf/module7/5.php?p=07#par4

Over van Dale. (n.d.). Retrieved april 4, 2011, from Van Dale: http://www.vandale.nl/vandale/overvandale

Risicoanalyse NEN1050. (n.d.). Retrieved juli 6, 2011, from Euronorm: http://www.euronorm.net/content/template2.php?itemID=556

Succesfactoren. (n.d.). Retrieved juli 8, 2011, from BTSG: http://www.btsg.nl/infobulletin/succesfactoren.html

Tech-FAQ. (n.d.). *Info over Active Directory*. Retrieved mei 2011, from Active Directory: http://www.tech-faq.com/active-directory.html

Tech-FAQ. (n.d.). *Info over Active Directory*. Retrieved mei 2011, from Active Directory: http://www.tech-faq.com/qp-content/uploads/2009/02/active-directory.png

UMCG. (n.d.). *Info over de geschiedenis van het UMCG*. Retrieved maart 2011, from UMCG: www.umcg.nl/NL/UMCG/overhetumcg/Page/defaults.aspx

LITERATUUR

Bemelmans, P. *informatiesystemen en automatisering zesde druk.*

C.T. de Groot, J. d. (2002). *Informatiekunde 2 ondernemen met informatie.* Groningen/Houten: Wolters-Noordhoff.

E.O.J. Jans, K. W.-N. (2007). *Grondslagen administratieve organisatie, deel A: algemene beginselen, 20e druk.* Groningen/Houten: Wolters-Noordhoff.

Fijneman, R. (2006). *IT-auditing en de prakijk.* Den Haag: Sdu Uitgevers bv.

N. Van Dam, J. M. (2005). *Een prakijkgerichte benadering van organisatie en management, vijfde druk.* Groningen: Wolters-Noordhoff bv Groningen/Houten.

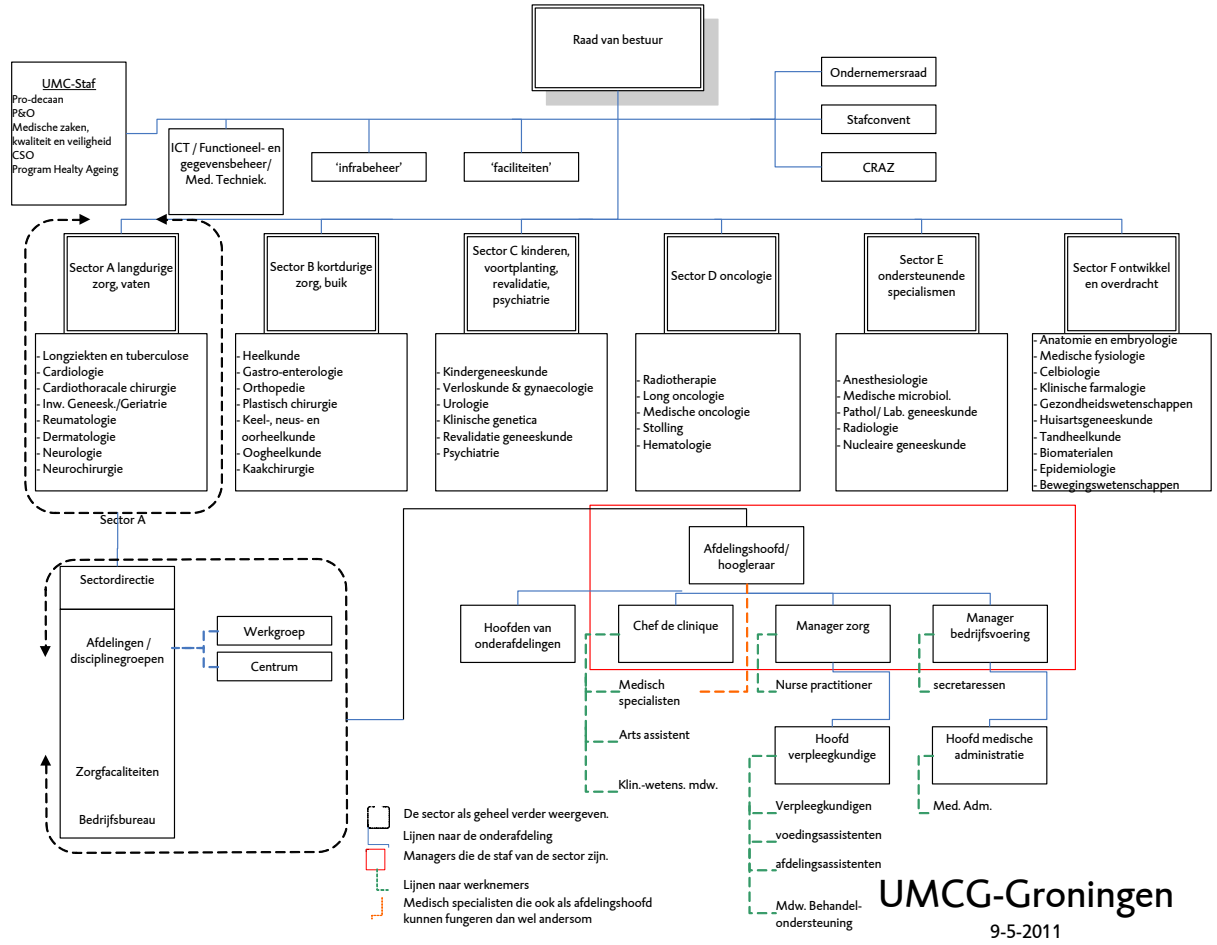
RAPPORTEN

FGB, B. (2010/2013). *Ontwikkelplan bureau FGB.* Groningen.

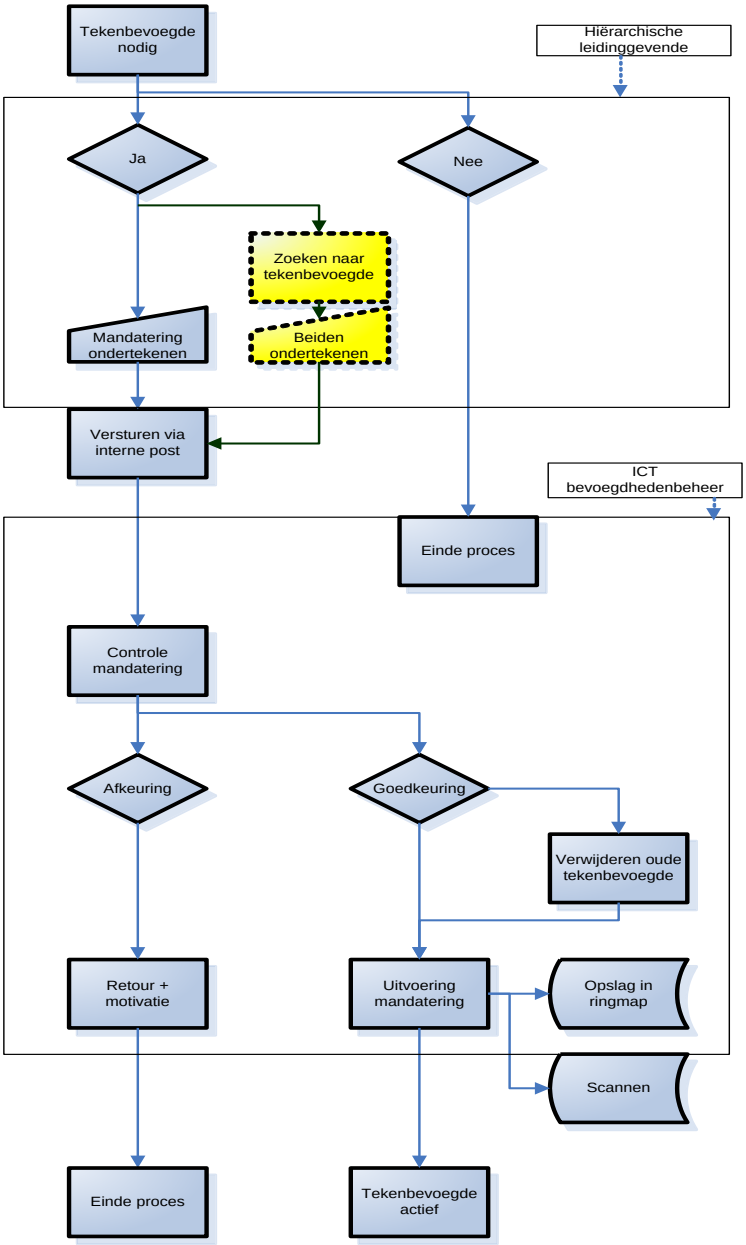
McKinsey&company. (2011). *Klaar voor de toekomst.*

Wenckebach Instituut. (n.d.). Retrieved februari 2011, from Wenckebach Instituut: www.wenckebachinstituut.nl

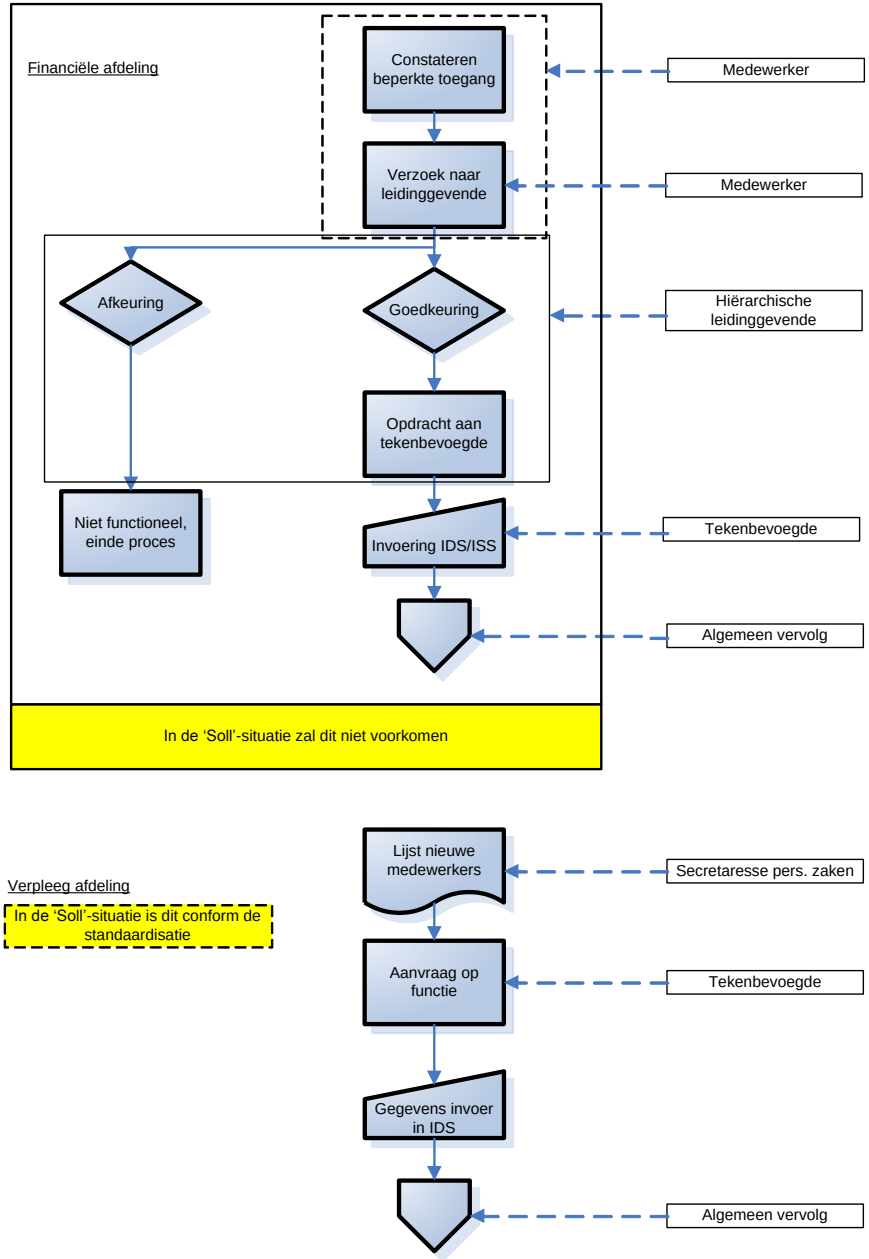
LIJST VAN FIGUREN



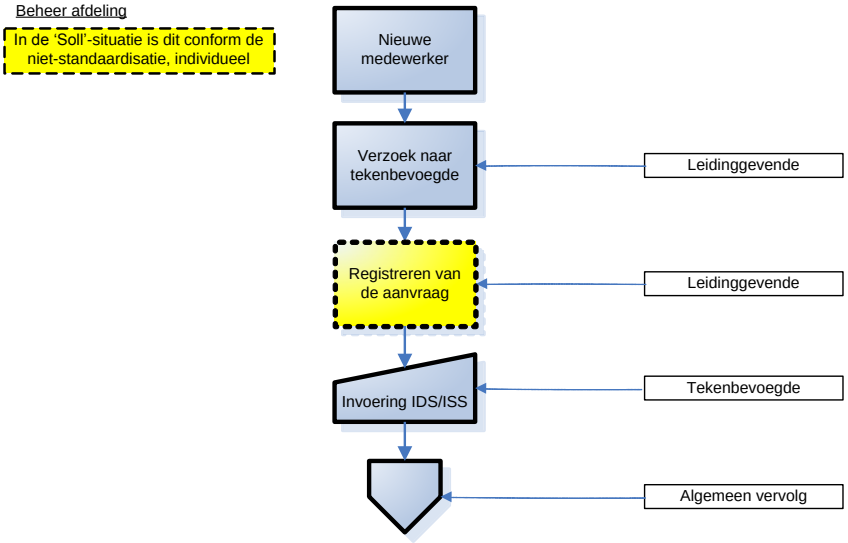
Figuur 10 Organisatiestructuur



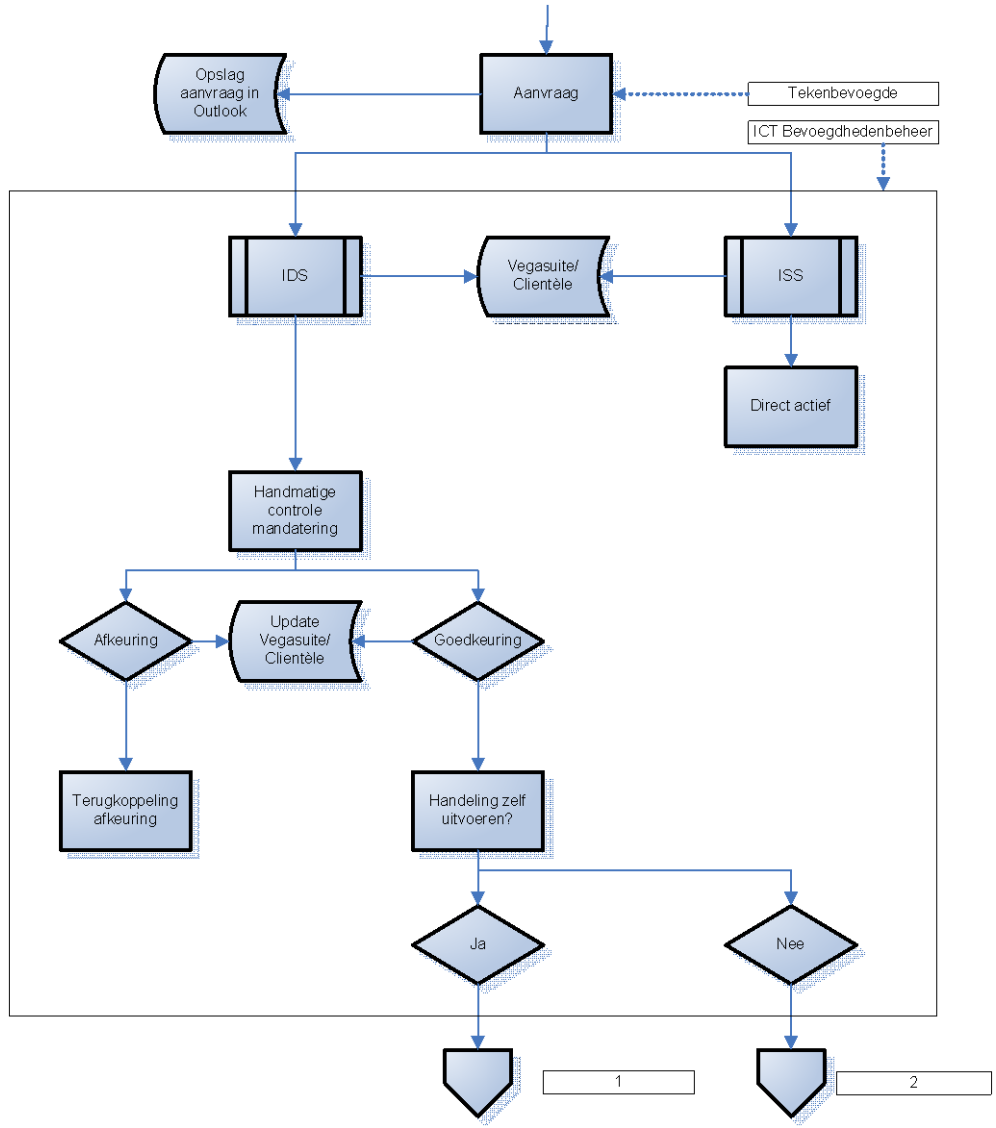
Figuur 11 De tekenbevoegde



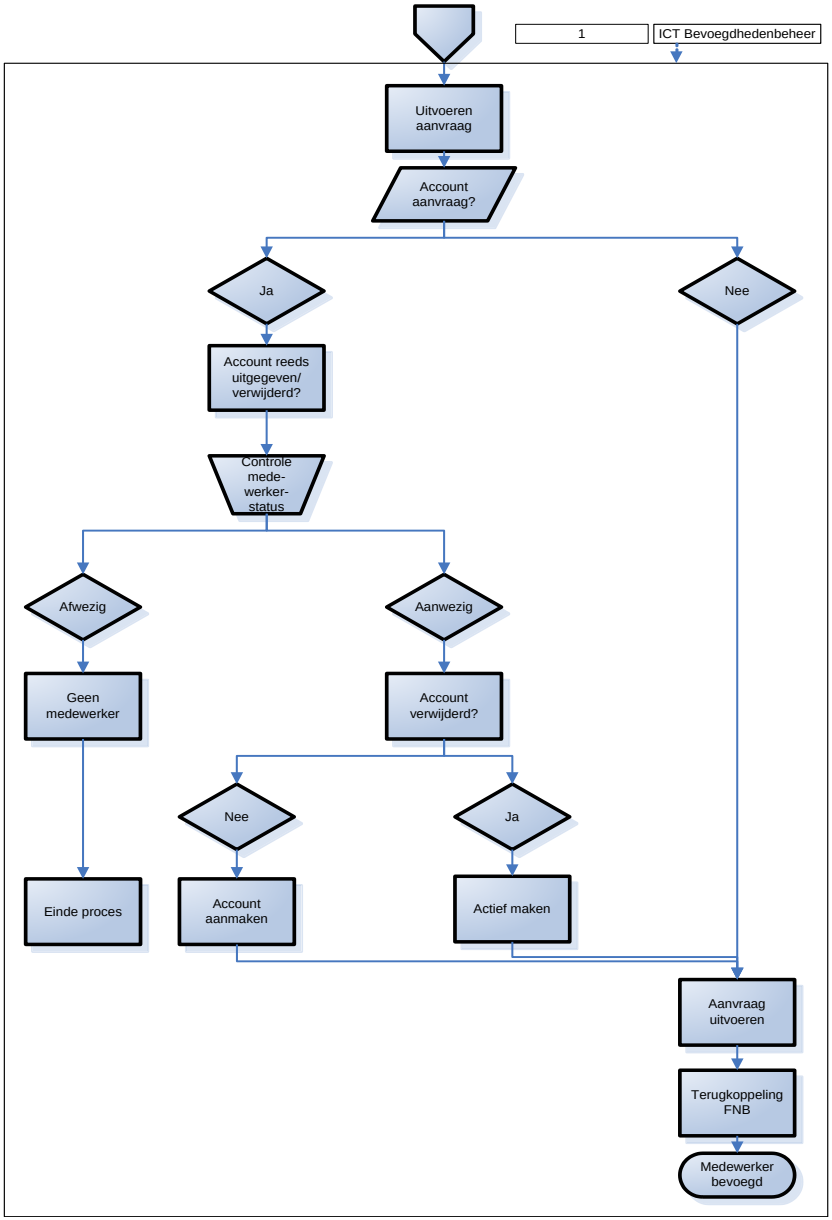
Figuur 12 Verstrekken van bevoegdheden op eigen afdeling



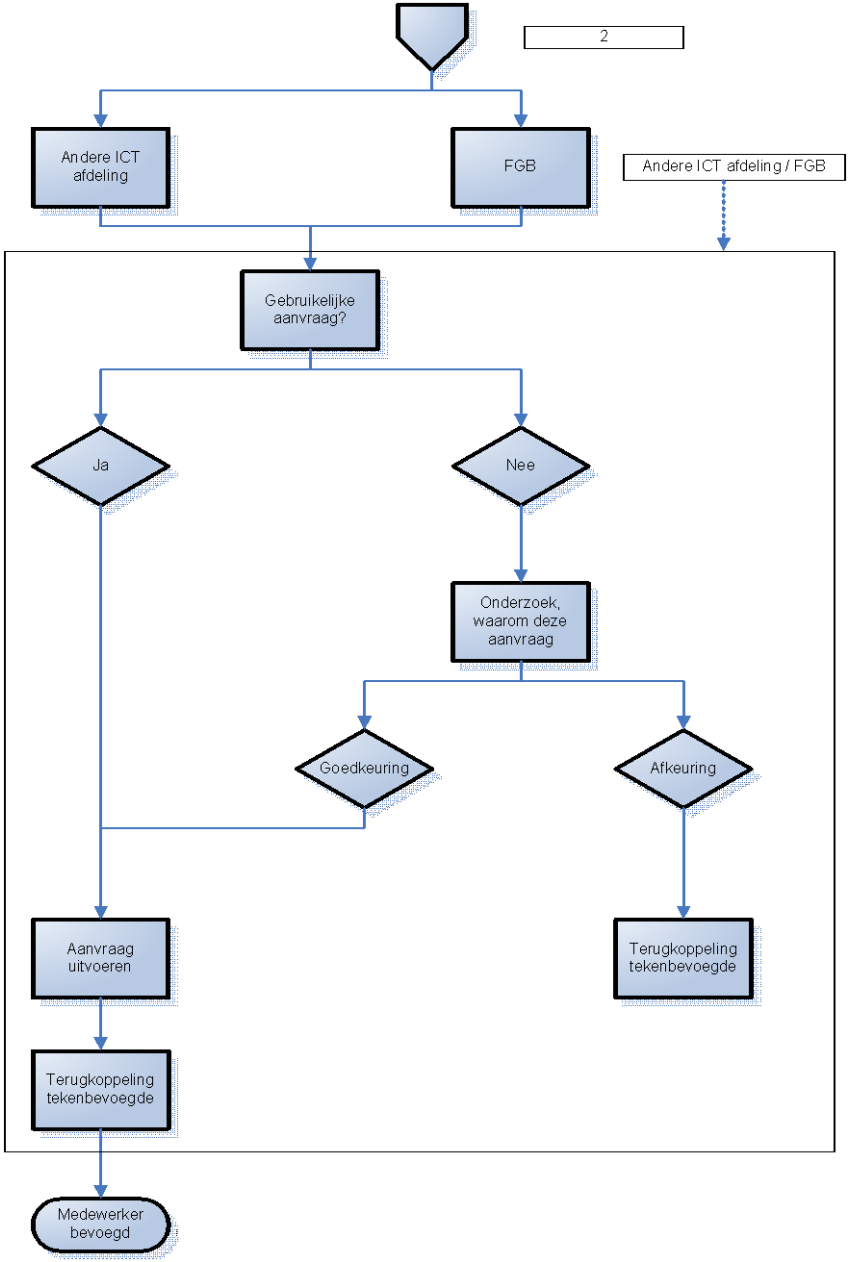
Figuur 13 Verstrekken van bevoegdheden op eigen afdeling



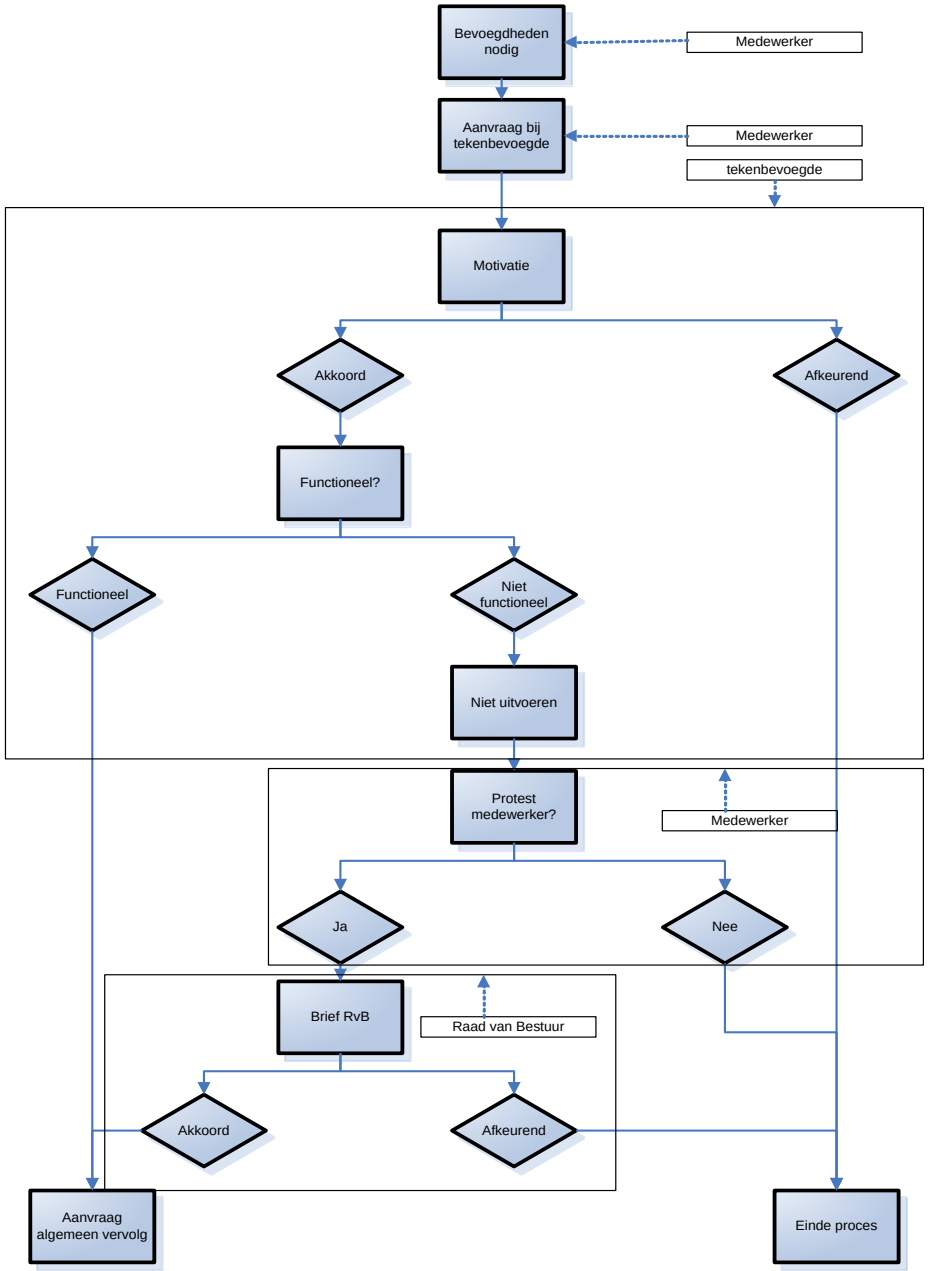
Figuur 14 Algemeen vervolg



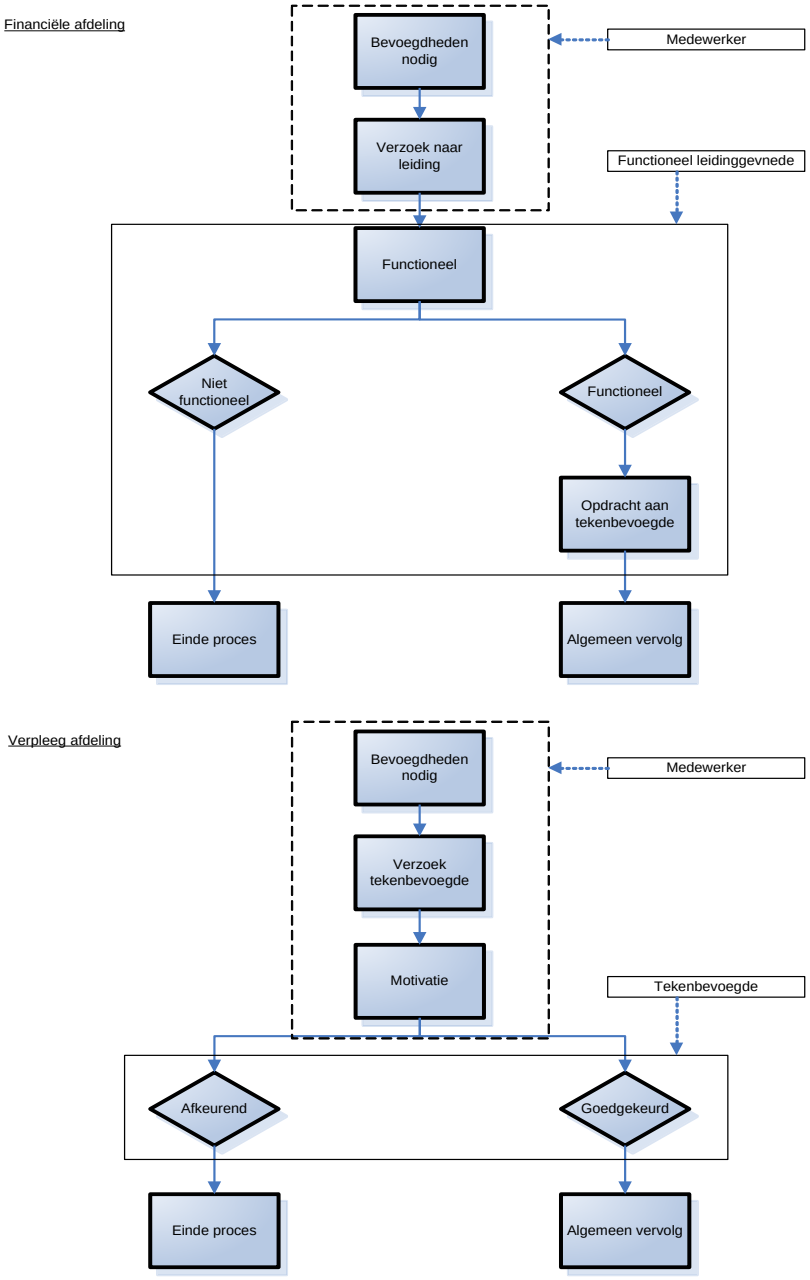
Figuur 15 Algemeen vervolg



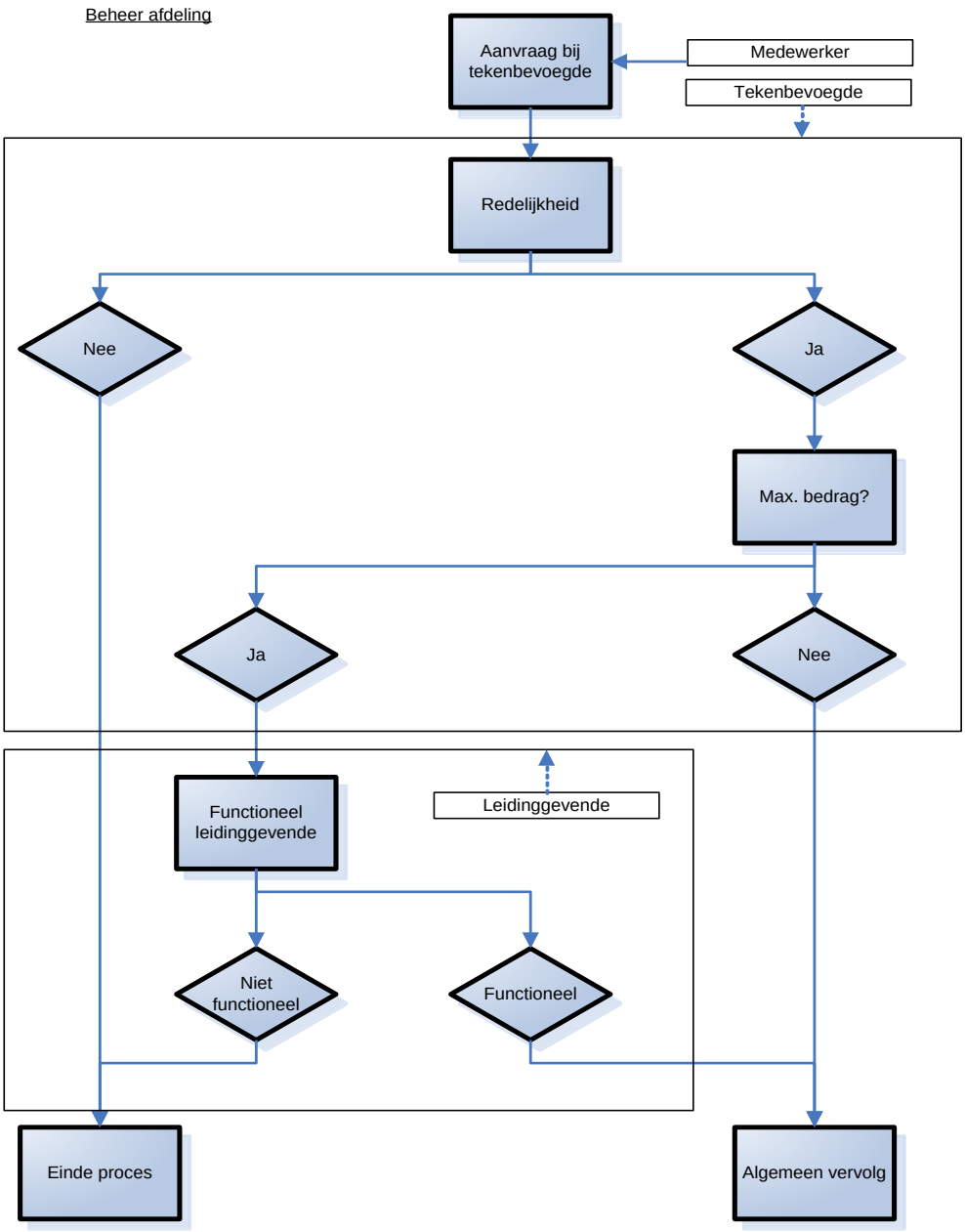
Figuur 16 Algemeen vervolg



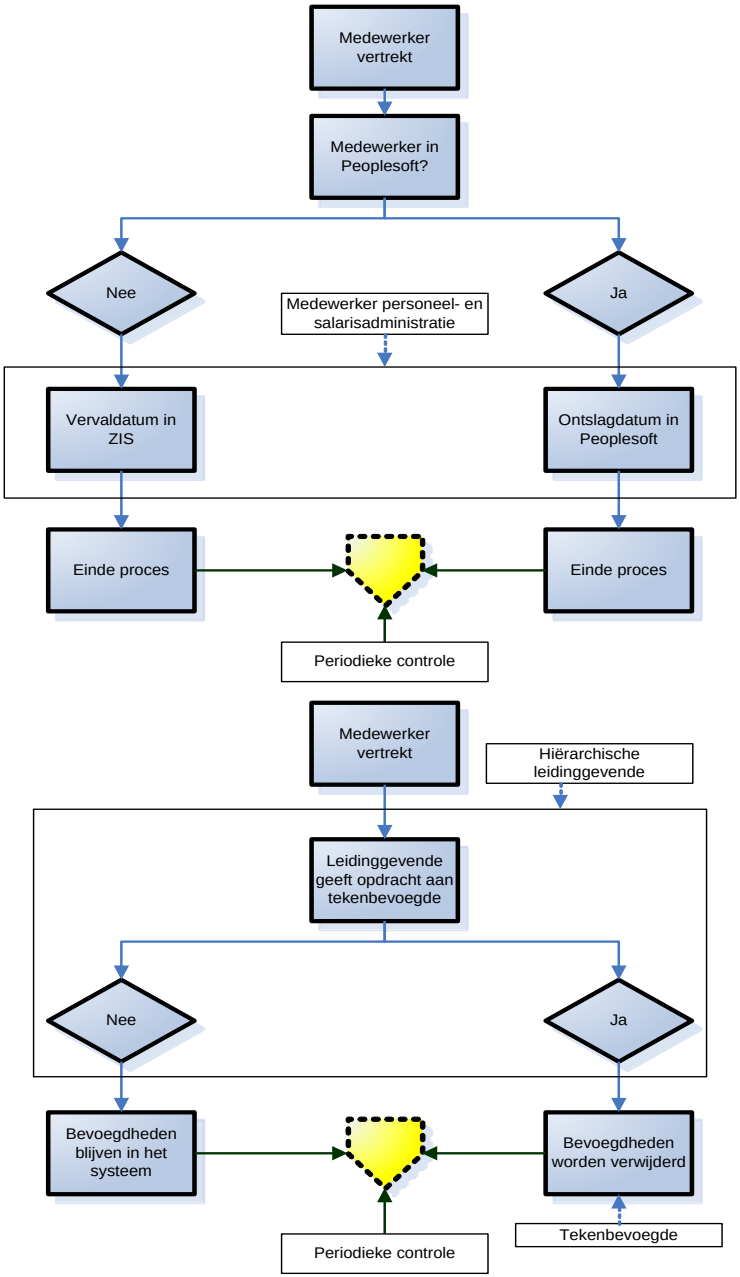
Figuur 17 Verstrekken bevoegdheden buiten eigen afdeling



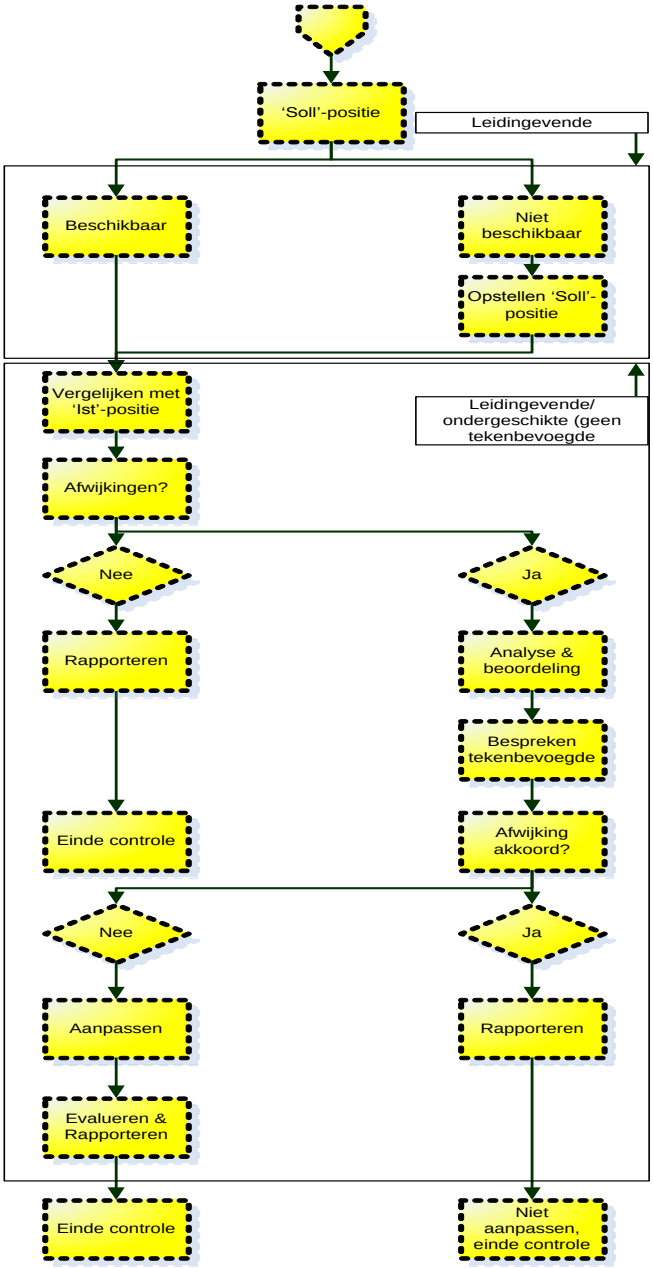
Figuur 18 Het uitbreiden/muteren van bevoegdheden



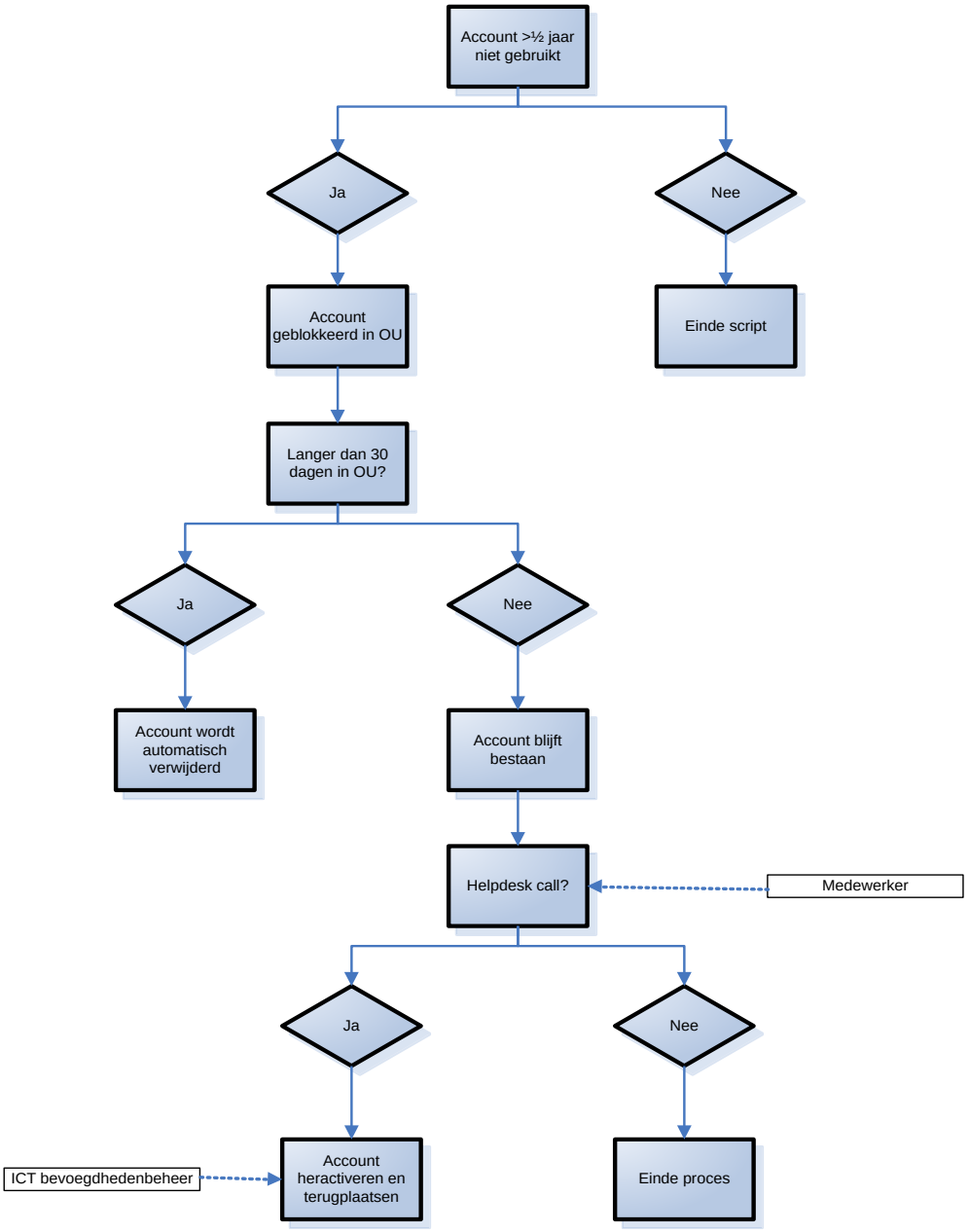
Figuur 19 Het uitbreiden/muteren van bevoegdheden



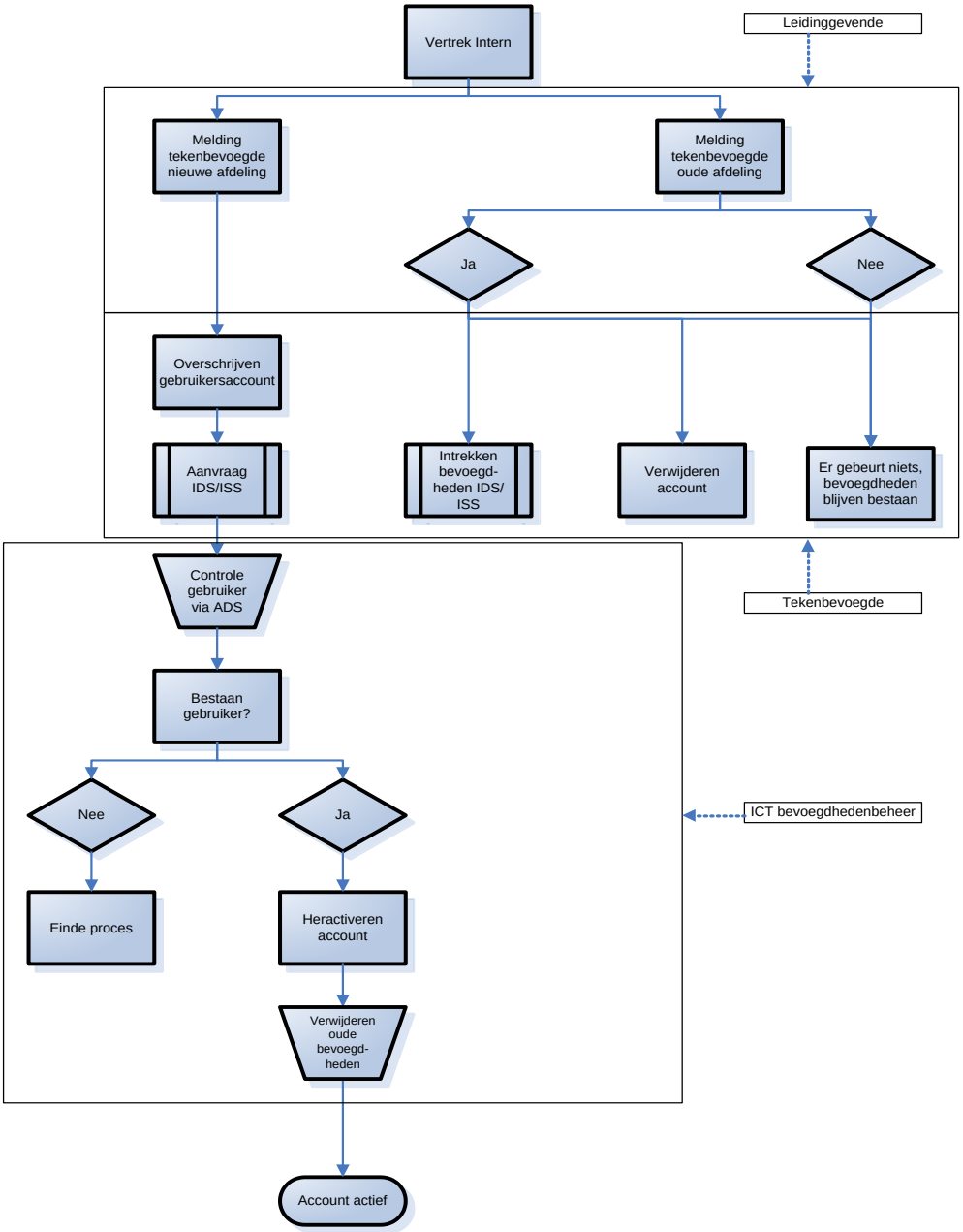
Figuur 20 Medewerker vertrekt extern



Figuur 21 Periodieke controle



Figuur 22 Script AD



Figuur 23 Intrekken bevoegdheden bij intern vertrek