**Role Based Access Control**

**Stop neglect.**

**Protect before you connect.**

****

Picture reproduced by permission from the Authors (David F. Ferraiolo, D. Richard Kuhn, Ramaswamy Chandramouli*)*

*Role-Based Access Control, Second Edition*, Norwood, MA: Artech House, Inc., 2006. © 2007 by Artech House, Inc.

****

**Role Based Access Control**

**Stop neglect.**

**Protect before you connect.**

***Auteur:***

Naam: Patrick Vaes

Studentnummer: 2158962

Datum: 01-06-2012

Versie: 1.0

***Opleiding:***

Onderwijsinstelling: Fontys Hogeschool

Opleidingsrichting: ICT Management & Security

Opleidingssoort: Deeltijd

Adres: Rachelsmolen 1

5612 MA Eindhoven R1

Telefoonnummer: 08850 77299

Afstudeerbegeleider: Dhr. R.M.J.W. van der Heijden

Afstudeerperiode: 01-02-2012 t/m 01-08-2012

***Organisatie:***

Naam bedrijf: Ciber Nederland B.V.

Adres: Burgemeester Burgerslaan 40B

5245 NH Den Bosch

Telefoonnummer: 040 232 90 90

Begeleiding: Senior Consultant - J. Weerts

Security Officer - Drs. Ing. B. Beens

Compliance Officer - Drs. J. Smets RE

Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door print-outs, kopieën, of op welke andere manier dan ook, zonder voorafgaande schriftelijke toestemming van Ciber Nederland B.V. © Patrick Vaes, 2012.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Ciber Nederland B.V. © Patrick Vaes, 2012.

**Versiebeheer:**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Versie:*** | ***Status:*** | ***Datum:*** | ***Opmerkingen:*** |
| 0.1 | Concept | 20-05-2012 | 1e concept. |
| 0.2 | Concept | 25-05-2012 | Inhoudelijke feedback Security Officer. |
| 0.3 | Concept | 29-05-2012 | Feedback op concept Dhr. Van der Heijden. |
| 0.4 | Concept | 31-05-2012 | Inhoudelijke feedback Compliance Officer. |
| 0.5 | Concept | 03-06-2012 | Inhoudelijke feedback Senior Consultant. |
| 1.0 | Final | 04-06-2012 | - |
|  |  |  |

**Goedkeuring:**

|  |  |  |  |
| --- | --- | --- | --- |
| ***Versie:*** | ***Status:*** | ***Datum:*** | ***Opmerkingen:*** |
| 1.0 | Final | 04-06-2012 | Senior Consultant J. Weerts |
|  |  |  |  |
|  |  |  |  |
|  |  |  |

**Verzendlijst:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Versie:*** | ***Status:*** | ***Datum:*** | ***Aantal:*** | ***Opmerkingen:*** |
| 1.0 | Final |  | 5 | Ciber Nederland B.V. |
| 1.0 | Final |  | 5 | Fontys Hogeschool ICT |
|  |  |  |  |  |
|  |  |  |  |  |

**Voorwoord**

Deze scriptie is geschreven ter afronding van de bachelorstudie Informatie en Communicatie Technologie (ICT) Management en Security (MS) aan Fontys Hogeschool te Eindhoven. Gedurende de periode dat ik bij Ciber Managed Services (CMS) mijn scriptie heb geschreven

is mijn leercurve op het gebied van ICT en dan met name de beveiliging ervan erg hoog geweest. Veel van wat beschikbaar is op het gebied van security zijn over het algemeen "best practices" en het is de kunst om de juiste invulling van de "best practices" te geven passend bij de organisatie.

Ondanks dat ik uit een compleet andere bedrijfscultuur kom, ben ik in staat gesteld om mijn ervaringen en mening te delen of te ventileren. Mijn gevoel hierbij is dan ook dat ik als een volwaardig collega gezien wordt die zijn specialisatie op het gebied van security aan het vervolmaken is.

De afstudeeropdracht Role Based Access Control (RBAC) voor CMS leek aanvankelijk een grote opdracht, die met een duidelijke structuur en werkwijze succesvol kon worden voltooid. Na een kleine oriëntatie kwam ik erachter dat RBAC voor zowel de organisatie als de theorie zelf, veel dieper gaat dan ik initieel in gedachte had. Na dieper in de materie RBAC gedoken te zijn, blijkt dat hier toch een aantal haken en ogen aan zitten. Het kan namelijk op verschillende manieren worden toegepast en is veel uitgebreider dan ik aanvankelijk in gedachten had.

Het beoogde effect van deze scriptie is de lezer meer inzicht te geven in het project RBAC voor CMS. In deze scriptie kan de basis gevonden worden van de theorie, verder onderzoek en implementatie van dit project binnen CMS en dan specifiek voor de afdelingen Networking & Storage en Servers. Ondanks dat het voltooien van dit project slechts een start is van de implementatie in zijn algeheel, heb ik veel plezier beleefd aan het schrijven van deze scriptie. Bovendien heb ik geleerd dat security in de wereld van ICT niet zo eenvoudig is als het lijkt.

Bij het schrijven van deze scriptie gaat mijn dank uit naar de medewerkers van CMS en scriptiebegeleiders. Voor deze scriptie waren dat er drie: Senior Consultant J. Weerts, Security Officer Drs. Ing. B. Beens en Compliance Officer Drs. J. Smets RE. Met hun kennis, advies en kritische houding hebben zij allen een waardevolle bijdrage geleverd aan deze scriptie. Gedurende het schrijven van deze scriptie heb ik geen enkele keer voor een gesloten deur gestaan. Daarnaast werd ik van informatie voorzien die voor mijzelf erg lastig te achterhalen was. Daarom wil ik alle begeleiders en medewerkers van CMS van harte bedanken voor hun inzet.

Patrick Vaes

juni 2012

# Samenvatting

Ciber Managed Services (CMS) is een full-service ICT dienstverlener die voor klanten de gehele of een gedeelte van de ICT omgeving in beheer neemt.Het is daarom voor CMS van groot belang dat de beschikbaarheid, integriteit en vertrouwelijkheid van haar informatiesystemen op een hoog niveau zijn. Dit met als doelstelling dat de veiligheidrisico's tot een minimum zijn teruggebracht.

Om invulling aan het beveiligingsbeleid te geven heeft CMS gekozen voor Role Based Access Control (RBAC) en dan specifiek de methode van het National Institute for Standards and Technology (NIST). Het doel van dit project is dus een generieke aanpak, met oog op de toekomst, te creëren die een groot aantal veiligheidsrisico's dekt. Aansluitend om deze vervolgens te implementeren en te borgen in de ICT omgeving en bedrijfsprocessen.

Voor dit project is een plan van aanpak (PVA) geschreven. De PVA is met een afgeleide methode van PRINCE 2 geschreven passend bij CMS. Deze methode heeft als resultaat dat het project op de juiste manier kan worden gestart. Het doel van de methode is een gedegen fundament voor het project RBAC.

De conclusie van dit project is dat door middel van de ontwikkelde template invulling gegeven kan worden aan het beveiligingsbeleid en het minimaliseren van de veiligheidsrisico's. De onderliggende doelstelling is tevens de teamleads geheel verantwoordelijk te laten over de realisatie hiervan middels de template. Dit alles gebeurd in combinatie met de functionele rol die bekend is binnen CMS.

Verder is het project nog steeds lopende en zal spoedig ook worden uitgevoerd op de overige afdelingen. Aansluitend hieraan zal gekeken worden of er diepgang naar de onderliggende lagen van het informatiesysteem plaats dient te vinden.

# Summary

Ciber Managed Services (CMS) is a full-service ICT service provider that manages and maintains part of or the whole IT environment of their customers. Therefore it is crucial that the confidentiality, integrity and availability of the IT environment is on a very high level. This with the ultimate goal of reducing the security risks to a minimum.

In order to give substance the security policy and reducing some of the security risks CMS has chosen for Role Based Access Control (RBAC) and specifically for the method from the National Institute for Standards and Technology (NIST). The goal of this project is a generic approach with an eye on the future that covers a large amount of security risks and will be implemented in the IT environment but also secure them in the business processes.

For the RBAC project there is an Project Initiation Document (PID). The PID is a derivative of the PRINCE 2 method that is suited for CMS. The purpose of the PID is that there is a solid foundation for this project with a result that it is initiated in a correct manner.

The conclusion of this project is that with the developed template, substance can be given to the security policy and minimize the security risks. Furthermore they will be warranted within the business processes. The underlying purpose is also to let the responsibility completely rest with the team leads in combination with the template. All this is done in arrangement with the functional role that is known within CMS.

Furthermore this project is still ongoing and soon shall be implemented in the other departments. To be followed by an evaluation if it is needed to expand this into the lower layers of the IT environment or keep it as it is.

**Inhoud**

[Samenvatting 5](#_Toc326342199)

[Summary 6](#_Toc326342200)

[1. Inleiding 8](#_Toc326342201)

[1.1 Het bedrijf 9](#_Toc326342202)

[1.2 Informatiebeveiliging 10](#_Toc326342203)

[1.3 Doelstelling 11](#_Toc326342204)

[1.4 Vraagstelling 11](#_Toc326342205)

[1.5 Structuur 11](#_Toc326342206)

[2. Procesbeschrijving RBAC project 12](#_Toc326342207)

[3. Theorie RBAC 14](#_Toc326342208)

[3.1 Flat RBAC 16](#_Toc326342209)

[3.2 Hierarchical RBAC 16](#_Toc326342210)

[3.3 Constrained RBAC 17](#_Toc326342211)

[3.3.1 Static Segregation of Duty 17](#_Toc326342212)

[3.3.2 Dynamic Segregation of Duty 18](#_Toc326342213)

[3.4 Symmetric RBAC 18](#_Toc326342214)

[4. Niveau keuze RBAC voor CMS 19](#_Toc326342215)

[4.1 Optie 1 - Flat RBAC 20](#_Toc326342216)

[4.2 Optie 2 - Hierarchical RBAC 22](#_Toc326342217)

[4.3 Optie 3 - Limited Static Constrained RBAC 24](#_Toc326342218)

[4.4 Optie 4 - Symmetric RBAC 26](#_Toc326342219)

[4.5 Opties gewogen 26](#_Toc326342220)

[5. Implementatie RBAC 28](#_Toc326342221)

[5.1 Huidige situatie met rechten en rollen 28](#_Toc326342222)

[5.2 Naamgevingconventie voor rollen 29](#_Toc326342223)

[5.3 Implementatie afdeling Networking & Storage 30](#_Toc326342224)

[5.4 Implementatie afdeling Servers 32](#_Toc326342225)

[6. Advies implementatie overige afdelingen 33](#_Toc326342226)

[6.1 Aanpak implementatie per afdeling 33](#_Toc326342227)

[7. Conclusies en aanbevelingen 35](#_Toc326342228)

[7.1 Conclusies 35](#_Toc326342229)

[7.2 Aanbevelingen 36](#_Toc326342230)

[8. Evaluatie 37](#_Toc326342231)

[Literatuur 39](#_Toc326342232)

[Geraadpleegde internetsites 39](#_Toc326342233)

[Afkortingenlijst 40](#_Toc326342234)

[Bijlage A Plan van aanpak 41](#_Toc326342235)

[Bijlage B Communicatieplan 60](#_Toc326342236)

**1. Inleiding**

Een goed en betrouwbaar informatiesysteem is voor elke organisatie onmisbaar. Dit geldt zowel voor commerciële als overheidsinstellingen. De structuur van het informatiesysteem kan daarbij sterk variëren. Voor sommige organisaties is een klein lokaal informatiesysteem voldoende, anderen hebben behoefte aan een informatiesysteem dat zich over de hele wereld uitspreidt.

Door de kosten van de interne ICT organisatie kan het een reden zijn om deze organisatie uit te besteden bij een ICT dienstverlener. Deze ICT dienstverleners hebben meerdere klanten in hun bestand en men onderhoud de dienstverlening van iedere klant naar de specifieke wensen en eisen. De dienstverlening kan inhouden van het beheren van de werkplekken tot het ontwikkelen van een klantgericht specifiek informatiesysteem. Globaal kan men zeggen dat het ICT dienstverlening is in de breedste zin van het woord.

De beveiliging van informatiesystemen is vaak gericht op risico's en invloeden van buitenaf en minder op interne invloeden. De interne invloeden kunnen in deze inhouden dat medewerkers onbewust op een verkeerd informatiesysteem werkzaamheden aan het verrichten zijn. Mogelijk zelfs tot het bewust uitzetten van een systeem wat niet wenselijk is. De impact van het ongecontroleerd uitzetten van een systeem of werkzaamheden op een verkeerd systeem kan leiden tot het verlies van klanten. Om ervoor te zorgen dat deze risico's zijn afgedekt zijn verschillende methoden en technieken toepasbaar. Zo is ondertussen standaard binnen verschillende informatiesystemen een scheiding in verantwoordelijkheid en toegang aangebracht. Het risico dat niet geautoriseerde personen toegang hebben tot deze informatiesystemen is daarmee verminderd.

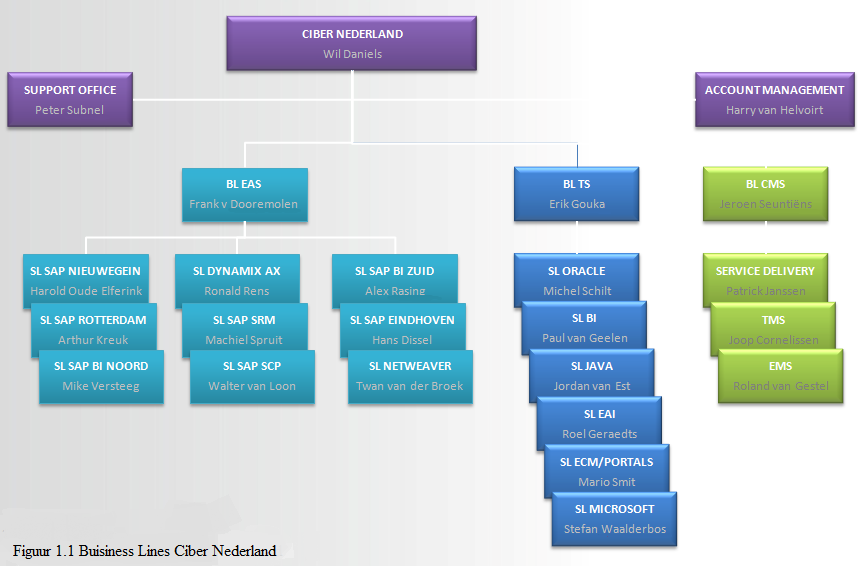
Dit project moet zorg dragen voor de ontwikkeling van een generieke methode. Deze methode is passend bij CMS, en is bedoeld om het aantal veiligheidsrisico's tot een minimum te reduceren. Deze generieke methode wordt vervolgens geïmplementeerd op de buitenste laag van het informatiesysteem. Het theoretisch kader waarvoor CMS heeft gekozen is Role Based Access Control (RBAC) en dan specifiek de variant die is ontwikkeld door het National Institute for Standards and Technology (NIST). Deze variant is gekozen omdat het systeem onafhankelijk toegepast kan worden. Verder is het een "best practice" en is tevens een verzameling van verscheidene theorieën. Men heeft ook in deze variant aangehaald dat deze nog aangepast dient te worden aan de bedrijfssituatie.

Het uiteindelijke doel van dit project is een gedegen aanpak en uitvoering geven aan het beveiligingsbeleid. Het beveiligingsbeleid zal uiteindelijk reflecteren richting de klanten van CMS en de dienstverlening naar een hoger niveau tillen.

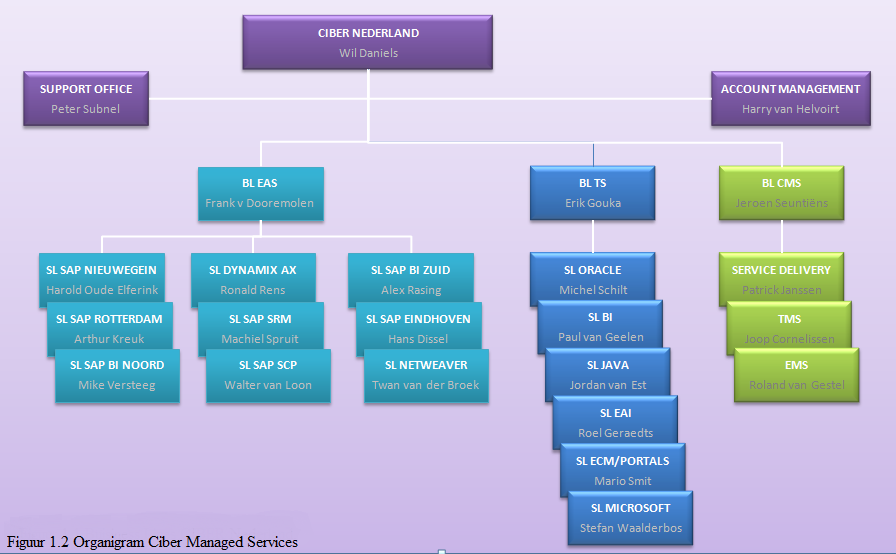
## 1.1 Het bedrijf

Ciber Incorporated is een full-service ICT dienstverlener ontstaan in 1974 met omzet van ongeveer 1,2 miljard USD in 2011 en beursgenoteerd op de New York Stock Exchange. Ciber Incorporated is een Gartner Tier 1 ICT dienstverlener met meer dan 9000 medewerkers verdeeld over 72 kantoren in 19 verschillende landen. Ciber Incorporated levert dienstverlening aan in zowel Onshore, Offshore als Nearshore locaties.

Ciber Nederland is ontstaan in 1996 met een omzet van ongeveer 100 miljoen Euro in 2011. Ciber Nederland heeft ongeveer 525 medewerkers verdeeld over 5 kantoren. Ciber Nederland richt haar dienstverlening in zowel Offshore als Nearshore en is "preferred supplier" van een groot aantal Nederlandse multinationals. Ciber Nederland is onderverdeeld in een aantal Business Lines zoals weergegeven in figuur 1.1.



De Ciber Managed Services tak bedient haar klanten door de ICT dienstverlening over te nemen van de klant of de voormalige ICT dienstverlener om zo de ICT systemen voor de klant te beheren. Tevens zijn alle specialiteiten die in de andere Business Lines (BL) vertegenwoordigd zijn ook aanwezig in de Ciber Managed Services tak. Een organigram van de Ciber Managed Services tak is in figuur 1.2 weergegeven.



## 1.2 Informatiebeveiliging

Beveiliging en beschikbaarheid van informatiesystemen is essentieel voor zowel commerciële als overheidsinstellingen. Als bedrijfskritische informatiesystemen niet meer beschikbaar zijn, kan dit leiden tot een strategisch nadeel en eventueel verlies van inkomsten. Uiteindelijk kan dit zelfs tot de ondergang van de commerciële of overheidsinstellingen leiden. Extreme beveiliging van informatiesystemen ten behoeve van de beschikbaarheid brengt echter ook een aantal nadelen met zich mee. De gebruiker zal steeds meer moeite moeten doen om te bewijzen dat hij of zij wel recht heeft op toegang tot informatie of een informatiesysteem. Het aantal gebruikers dat toegang heeft tot bepaalde informatiesystemen zal mogelijk kleiner kunnen worden. Het resultaat kan zijn dat mensen hun werk niet meer goed kunnen uitvoeren of er teveel tijd voor nodig hebben. Een balans moet gezocht worden tussen veiligheid en werkbaarheid van een informatiesysteem om de beschikbaarheid en integriteit te garanderen. Vooral bij ICT dienstverleners is sprake van meerdere informatiesystemen omdat, men deze tenslotte beheerd voor de klanten. Elk informatiesysteem maar ook elke klant stelt andere eisen op het gebied van informatiebeveiliging. De beveiliging dient op een zodanige wijze toegepast te worden, dat informatiesystemen van verschillende klanten indien gewenst gescheiden blijven maar dat ook de beschikbaarheid en integriteit gegarandeerd is.

Een model waarbij de risico's van informatiesystemen bij een ICT dienstverlener kunnen worden verminderd zodat de integriteit en beschikbaarheid blijven gewaarborgd is via het National Institute for Standards and Technology (NIST) Role Based Access Control (RBAC) model ontwikkeld en geschreven door de heren Ravi Sandhu, David Ferraiolo en Richard Kuhn. Dit document heeft als titel: "The NIST model for Role Based Access Control: Towards a Unified Standard" en is geschreven in het jaar 2000. In deze scriptie wordt niet gezocht of het model het beste is. Er wordt juist gezocht naar een generieke manier van toepassen en implementeren met oog op de toekomst.

## 1.3 Doelstelling

De doelstelling van dit onderzoek is tweeledig. Ten eerste heeft dit onderzoek het doel om te kijken of het mogelijk is om Role Based Access Control (RBAC) in te voeren binnen Ciber Managed Services (CMS) op de afdelingen Networking & Storage en Servers. Ten tweede zal het onderzoek duidelijkheid verschaffen over de beste keuze van invoering op de overige afdelingen van CMS.

## 1.4 Vraagstelling

De hoofdvraag voor dit onderzoek luidt als volgt: ,,Hoe kan het RBAC model worden toegepast op de afdelingen Infrastructure & Storage en Servers van een Managed Service organisatie?” Vanuit deze hoofdvraag kunnen een aantal onderzoeksvragen worden afgeleid:

* Wat is het RBAC model?
* Wat is het doel van RBAC?
* Tot welk niveau gaat RBAC geïmplementeerd worden?
* Wat zijn de voordelen?
* Wat zijn de nadelen?
* Is implementatie op de overige afdelingen mogelijk?

## 1.5 Structuur

De kern van deze scriptie bestaat globaal uit zes delen:

* **Hoofdstuk 2: Procesbeschrijving RBAC project.** In dit hoofdstuk is een globale beschrijving gegeven over de invulling van het RBAC project.
* **Hoofdstuk 3: Theorie RBAC model**. In dit hoofdstuk wordt de theorie van RBAC beschreven. Daarnaast staat in dit hoofdstuk het doel van RBAC beschreven.
* **Hoofdstuk 4: Niveau keuze RBAC.** In dit hoofdstuk worden de verschillende mogelijke niveaus beschreven voor RBAC. Tevens wordt gekeken welk niveau het beste past bij Ciber Managed Services.
* **Hoofdstuk 5:** **Implementatie RBAC.** In dit hoofdstuk wordt beschreven hoe vorm gegeven word aan RBAC binnen CMS.
* **Hoofdstuk 6: Advies implementatie overige afdelingen.** In dit hoofdstuk wordt een advies gegeven over de invoering op de overige afdelingen.
* **Hoofdstuk 7: Conclusies en aanbevelingen.** In dit hoofdstuk wordt een advies gegeven over hoe nu verder met oog op de toekomst en de verdere invoering RBAC.

Na het bestuderen van deze hoofdstukken zal het project RBAC voor CMS inzichtelijk zijn gemaakt. Als laatste zal een evaluatie volgen die gericht is op de projectleider om inzicht te verschaffen over de knelpunten en successen die bij dit project zijn gerezen of behaald.

# 2. Procesbeschrijving RBAC project

In dit hoofdstuk volgt een globale beschrijving en de gebruikte onderzoeksmethoden van het RBAC project. Het RBAC project is, na goedkeuring van het plan van aanpak (PVA), gestart door middel van een aantal vergaderingen. Deze vergaderingen hadden als doel om een detailinvulling te geven aan de eisen en beperkingen van het RBAC project.

De eisen en beperkingen van dit project zijn hieronder genoemd met de detailinvulling:

***Eis:*** *Uitvoer geven aan het beveiligingsbeleid en tevens de risico's voor de klanten en CMS zoveel mogelijk verminderen.*

***Details:*** Een gedegen onderzoek en de creatie van een generieke aanpak (template) middels de RBAC methode vermindert de risico's maar zal ook het autorisatie proces met betrekking tot rechten en rollen transparant maken.

***Eis:*** *Kwaliteit verhogen richting de dienstverlening naar de klant.*

***Details:*** Het RBAC project zal leiden tot transparantie met betrekking tot de veiligheid van de informatiesystemen wat de kwaliteit verder verhoogd.

***Eis en beperking:*** *Kostenefficiënt invulling geven aan de invoer van RBAC.*

***Details:*** Alleen op aanvraag en na goedkeuring van de Senior Consultant worden andere medewerkers belast met werkzaamheden voor dit project.

***Beperking:*** *Operationele activiteiten mogen niet worden verstoord.*

***Details:*** Een manier zal onderzocht moeten worden voor de implementatie van het RBAC project. Het RBAC project zal synchroon aan de huidige situatie geïmplementeerd moeten worden, omdat de operatie anders verstoord wordt.

Aansluitend aan de detailinvulling van de eisen en beperkingen is het onderzoek van start gegaan. Het onderzoek is gedaan middels twee kwalitatieve onderzoeksmethoden namelijk een literatuuronderzoek en open interview (vergadering). Het literatuuronderzoek heeft voornamelijk als doel de gekozen methode van RBAC te onderzoeken. Bij het literatuuronderzoek is de toepasbaarheid van de theorie naar de organisatie onderzocht. Aansluitend aan het literatuuronderzoek is doormiddel van open interviews (vergaderingen) de beleving gezocht zoals de teamleads invulling willen geven aan het RBAC project.

Het onderzoek leidt tot een aantal mogelijke opties met betrekking tot de generieke aanpak (template) en implementatie van RBAC. De opties worden beschreven in een adviesrapport en vervolgens gepresenteerd aan de Senior Consultants van CMS. De presentatie heeft als voornaamste doel om een keuze te maken uit de mogelijke opties. Eveneens is de presentatie de ideale mogelijkheid om draagvlak te creëren bij de medewerkers van CMS.

De volgende fase van het RBAC project is om invulling te geven aan de gekozen oplossing. De template wordt samen met de teamlead van de desbetreffende afdeling ingevuld. Indien benodigd wordt een test- en implementatieplan geschreven voor de desbetreffende afdeling. Als de template compleet, naar de behoeften en wensen van de teamlead, is ingevuld wordt een vergadering belegd met een specialist van de afdeling Servers. De vergadering heeft als doel de template synchroon bij de huidige situatie van de afdeling te implementeren.

Tijdens de implementatie wordt een medewerker aan de gecreëerde rol gekoppeld en deze wordt vervolgens getest. De teamlead bepaald de tijdsduur in dagen van testen en wanneer geen verstoringen hebben opgetreden volgt het omzetten van de gehele afdeling naar de nieuwe situatie. De oude situatie blijft dan nog een door de teamlead te bepalen tijdsduur in dagen staan en wordt aansluitend geschoond.

Aansluitend aan de implementatie volgt een evaluatie van de rechten die gekoppeld zijn aan de rollen. De evaluatie heeft als doel om te controleren of de rechten die gekoppeld zijn aan de rollen de beveiligingsrisico's verminderen en voldoen aan de wensen van de teamlead.

Wanneer de evaluatie is voltooid volgt de borging van de rollen. De rollen worden geborgd door een beschrijving van de rollen te maken die door de teamlead wordt samengesteld per afdeling. De beschrijving wordt vervolgens opgenomen als een onderdeel van het beveiligingsbeleid. Met de beschrijving wordt men in staat gesteld om deze in de toekomst te controleren en auditen.

# 3. Theorie RBAC

Als ICT dienstverlener heeft men te maken met toegang tot verschillende ICT omgevingen zowel bij klanten als intern. Om ervoor te zorgen dat de risico's geminimaliseerd zijn, gebeurd dit door middel van het beperken van toegang en het toekennen van rechten via een standaard methode. De methode die hieruit is ontstaan noemt men Role Based Access Control (RBAC). Deze methode is op alle systemen toepasbaar alleen de mate waarin is per systeem afhankelijk.



RBAC is een manier om bepaalde risico's van toegang tot een informatiesysteem te verminderen. Het RBAC model is erop ingericht om op een zo efficiënte en effectieve wijze te implementeren zodat het beheersbaar blijft. Het belangrijkste eigenschap van RBAC is dat individuen rechten krijgen door een vorm van groepslidmaatschap. Individuen krijgen geen directe autorisatie tot informatiesystemen.

De vorm van groepslidmaatschap wordt op basis van de functie of rol die het individu binnen een organisatie of bedrijfsproces vervult. Ook de rechten op objecten/functies in informatiesystemen kunnen gegroepeerd worden in rollen. Door het toewijzen van een rol of meerdere rollen aan een individu is het overzichtelijk om de effectieve rechten te bepalen van het individu.

Een voorbeeld van een methode om RBAC te implementeren is om rollen te creëren naar aanleiding van de functies of rollen die voorkomen binnen de organisatie of bedrijfsproces. Een basis is namelijk benodigd om dit gecontroleerd te laten gebeuren zonder dat men de operatie frustreert. Deze rollen kunnen worden vastgesteld en vervolgens gecreëerd door middel van Role-mining. Role-mining is een techniek om de rechten van een gebruiker in kaart te brengen middels een analyse of proces.

Role-mining kan uitgevoerd worden op drie manieren zijnde:

* Bottum-up;
* Top-down;
* By-example.

Bottum-up is het koppelen van gebruikers aan reeds bestaande rollen gebaseerd op hun vaardigheden en taken. De reeds bestaande rollen hebben een definitie. De definitie van de rollen zijn te vertalen in vaardigheden en taken. De vaardigheden en taken worden vergleken met de gebruiker die ook vaardigheden en taken bezit. Wanneer bij de vergelijking voor een bepaald percentage een overeenkomst is gevonden kan men de gebruiker aan de desbetreffende rol koppelen. Aansluitend zal een evaluatie van de rechten van de gebruiker en de rol volgen voor de rechten die niet overeenkomen. De evaluatie moet vervolgens inzicht verschaffen over het mogelijk ontnemen, behouden of toekennen van de rechten die niet overeenkomen. Indien dit geheel gereed is kan men de rechten van de gebruiker ontnemen en verkrijgt de gebruiker de rechten via de rol waaraan hij gekoppeld is.

Met top-down worden rollen geformuleerd door ze te matchen aan de vaardigheden en taken van de individuele gebruiker. De rollen worden geformuleerd middels een evaluatie van de taken en vaardigheden van de gebruiker. De evaluatie produceert een set rechten die de rol vormt. Vervolgens wordt de gebruiker aan de rol gekoppeld. De rechten gekoppeld aan de gebruiker worden aansluitend verwijderd. De gebruiker verkrijgt nu de rechten via de geformuleerde rol.

By-example is het koppelen van rollen aan gebruikers zoals deze zijn gedefinieerd door de managers. De definitie van de rollen worden hiërarchisch bepaald en men kan bijvoorbeeld een boomstructuur creëren of een indeling maken naar aanleiding van een organigram van de organisatie. De rechten die een rol krijgt zijn eveneens bepaald door de managers. De gebruikers worden aansluitend gekoppeld aan de rollen conform het functieprofiel van de organisatie. De rechten gekoppeld aan de gebruikers worden vervolgens verwijderd.

Men kan natuurlijk ook een combinatie van de drie mogelijke manieren van role-mining gebruiken.

Een voorkomend gebruikt model wat wordt toegepast is het National Institute Standards and Technology (NIST) RBAC model. Dit model is een "best practice" waar verschillende ideeën en visies bij elkaar komen.

Binnen het NIST RBAC model zijn vier niveaus te onderkennen:

* Flat RBAC
* Hierarchical RBAC
* Constrained RBAC
* Symmetric RBAC

De vier niveaus zijn cumulatief, met steeds meer functionele mogelijkheden en steeds wordt een nieuwe specificatie toegevoegd. Uitleg van ieder niveau is in de volgende subparagrafen beschreven.

## 3.1 Flat RBAC

In figuur 3.1 is een voorbeeld weergegeven van Flat RBAC. Flat RBAC belichaamt de essentiële aspecten van RBAC. Het basisconcept van RBAC is dat gebruikers worden toegewezen aan rollen, de rechten zijn toegekend aan rollen en gebruikers verwerven rechten door lid te zijn van rollen.

Het RBAC model vereist dat de user-rol en de permission-role toewijzing many-to-many kan zijn. Dus een gebruiker kan worden toegewezen aan een groot aantal rollen en een rol kan heel veel gebruikers hebben.



## 3.2 Hierarchical RBAC

In figuur 3.2 is een voorbeeld weergegeven van Hierarchical RBAC. Hierarchical RBAC voegt de specificatie voor rol hiërarchie toe ten opzichte van Flat RBAC. De hiërarchie in deze wordt gedefinieerd door een anciënniteit relatie tussen de rollen, waarbij de senior rollen de permissies van de junior rollen verwerven. Het RBAC model kent twee subniveaus in dit opzicht zijnde:

* **General Hierarchical RBAC:** In general hierarchical RBAC is ondersteuning voor een willekeurige gedeelte waaraan we rol hiërarchie kunnen opleggen. Men bepaald dus zelf tot op welk niveau en in welke omgeving rol hiërarchie toepast.
* **Restricted Hierarchical RBAC:** In restricted hierarchical RBAC kunnen sommige systemen beperkingen opleggen aan de rol hiërarchie zoals Microsoft Windows Server Edities en LINUX varianten. De toegevoegde waarde van dit soort systemen is dat men de mogelijkheid heeft gecreëerd om een verkapte vorm van RBAC toe te passen. Meestal wordt bij deze systemen de verkapte vorm van RBAC beperkt tot eenvoudige structuren zoals boomstructuur of omgekeerde boomstructuur.



## 3.3 Constrained RBAC

Constrained RBAC voegt als specificatie beperkingen toe aan hierarchical RBAC. Deze beperkingen zijn vooral gericht op de scheiding van taken en privileges (functies). Dit vooral om te voorkomen dat een gebruiker teveel rechten op een systeem kan krijgen waardoor mogelijk belangenverstrengelingen ontstaan. Het RBAC model kent hierin twee methoden en laat open welke van de twee ondersteund zou moeten worden. De twee methoden zijn verderop beschreven.

## 3.3.1 Static Segregation of Duty

In figuur 3.3 is een voorbeeld weergegeven van Constrained RBAC - STATIC Segregation of Duties (SOD). Belangenverstrengelingen in een role based access systeem kan ontstaan als gevolg van het verkrijgen van toestemming voor rechten geassocieerd met tegenstrijdige rollen. Een methode om deze vorm van belangenverstrengelingen te voorkomen is Static Segregation of Duty (SSD). Dit is het beperken van toekenning van gebruikers aan rollen. Dit houdt in dat als een gebruiker toegelaten word als lid van een rol, de gebruiker verboden is lid te zijn van een tweede rol.



## 3.3.2 Dynamic Segregation of Duty

In figuur 3.4 is een voorbeeld weergegeven van Constrained RBAC - DYNAMIC SOD. RBAC bied beheerders de mogelijkheid om bij een organisatie een specifiek beleid van Dynamic Segregation of Duty (DSD) af te dwingen. Met DSD is het toegestaan voor een gebruiker om toegelaten te worden als lid van een set rollen die geen belangenverstrengelingen opleveren als men hierin onafhankelijk van elkaar handelt. Deze produceren wel beleidskwesties wanneer hierin tegelijk word gehandeld. Zo kan een gebruiker erkend zijn voor de rol van kassier en van kassiersupervisor in gevallen waarbij de supervisor is toegestaan om correcties op een open kassalade te autoriseren. Als het individu handelend in de rol van kassier probeert over te schakelen naar de rol van kassiersupervisor zou RBAC het individu moeten dwingen de rol van kassier te laten vallen. Hiermee wordt de kassa gesloten en vervolgens kan men de rol van kassiersupervisor aannemen.



## 3.4 Symmetric RBAC

In figuur 3.5 en figuur 3.6 zijn voorbeelden weergegeven van respectievelijk Symmetric RBAC - STATIC SOD en Symmetric RBAC - DYNAMIC SOD. Het beheren en onderhouden van rollen is een essentieel onderdeel van ieder autorisatieschema. Rollen kunnen veranderen als situaties binnen een organisatie veranderen en nadelig zijn voor de beleidsdoelstellingen van een organisatie. Het beheren en onderhouden van rollen kan zelfs problematisch zijn als rechten zijn toegekend over verschillende informatiesystemen en een gecoördineerde inspanning van meerdere administrators een noodzaak is. Om hier effectief invulling aan te geven moet het mogelijk zijn om de rollen te herzien ongeacht op welk niveau deze binnen de organisatie zitten. Bij het onderhouden van rechten op rollen dient speciale aandacht gegeven te worden aan het toekennen van de minste-rechten-principe.

Dit principe houdt in dat een gebruiker alleen die rechten toegewezen krijgt, die essentieel zijn voor het werk van de gebruiker. De uitdaging wordt dan het toekennen van de rechten zodat het individu die wordt gekoppeld aan de rol, zijn functionele taken of werkzaamheden binnen de organisatie kan uitvoeren. Symmetric RBAC is een methode waarbij dit geautomatiseerd is. Dit wil zeggen dat alle rollen, rechten en relaties in kaart worden gebracht zonder dat men dat zelf hoeft uit te zoeken. Hierin zijn twee methoden te onderkennen namelijk Symmetric RBAC - STATIC SOD en Symmetric RBAC - DYNAMIC SOD. Beide zijn vanuit het vorige niveau een opvolging.





# 4. Niveau keuze RBAC voor CMS

In dit hoofdstuk worden de mogelijke opties met betrekking tot niveau keuze voor RBAC besproken. De uiteindelijke keuze is een beslissing die is gemaakt door het Management Team (MT) en is gebaseerd op de criteria die zijn gesteld voor dit project. Tevens is er gekeken of de basisfunctionaliteiten van RBAC een verbetering zijn van de huidige situatie bij CMS.

Voor de opties 1 tot en met 3 die verderop zijn beschreven is een template ontwikkeld die als basis wordt gebruikt bij de definitie van rollen. De template is dus de basis die inzicht verschaft over de totstandkoming van de rollen.

De eisen die bij dit project zijn gesteld zijn:

* Kostenefficiënt;
* Risico dekkend;
* Beheersbaar;
* Kwaliteitsverhogend;
* Acceptabel binnen CMS.

## 4.1 Optie 1 - Flat RBAC

Het invoeren van niveau één (Flat RBAC) van het RBAC model. In figuur 4.1 is de template weergegeven van deze optie. Flat RBAC houdt in dat rollen gecreëerd moeten worden ten behoeve van de functionaliteiten over de verschillende afdelingen. De beste manier om deze rollen tot stand te laten komen is via de bottum-up methode. De bottum-up methode zorgt dat de operatie niet gestoord wordt door de creatie van rollen. Informatie vergaren over de rollen zal inhouden een uitdraai te maken van de Active Directory (AD) om deze vervolgens te sorteren aan de hand van de functionaliteiten die functie behoord te hebben. Indien dit bij de twee afdelingen Networking & Storage en Servers is gebeurd, worden rollen gecreëerd voor de verschillende functionaliteiten. Als laatste zullen de medewerkers gekoppeld worden aan de rollen die men behoort te hebben.

De voordelen van deze methode zijn dat de huidige operatie vrijwel geheel al conform niveau 1 is ingericht op de creatie van rollen na. Ook is deze methode makkelijk uit te bereiden of te verkleinen indien gewenst. Tevens is voor deze methode geen extra software of programmatuur benodigd.

De nadelen van deze methode zijn dat nog steeds geen duidelijkheid wordt geboden in de structuur, waardoor controle en beheer moeilijk wordt. Tevens is deze methode is ook erg onderhevig aan wildgroei, omdat men niet duidelijk inzicht heeft in de rechten die aan de rollen zijn gekoppeld. De kans op dubbele rollen neemt door het beperkte inzicht toe. Het onderhoud van deze methode kan een tijdrovend geheel worden wat naar mate van tijd alleen maar toeneemt. Door deze methode blijft het met betrekking tot security dan ook een vraagstuk, of de werkzaamheden uitgevoerd kunnen worden door een medewerker, die de operatie als hoofdtaak en security als neven taak heeft. Ook de vraag of dit geheel risicodekkend is blijft bestaan.

***Voordelen:***

* Makkelijk te implementeren;
* Gemakkelijk uitbreidbaar of te verkleinen;
* Geen extra programmatuur of software nodig.

***Nadelen:***

* Geen duidelijkheid in de structuur;
* Niet gemakkelijk te controleren;
* Snel onderhevig aan wildgroei;
* Mogelijk dubbele rollen;
* Tijdrovend met betrekking tot onderhoud;
* Medewerker hoofdtaak operatie en neventaak security?
* Geheel risico dekkend?



## 4.2 Optie 2 - Hierarchical RBAC

Het invoeren van niveau één en twee (Hierarchical RBAC) van het RBAC model. In figuur 4.2 is de template weergegeven van deze optie. Hierarchical RBAC houdt in dat rollen gecreëerd moeten worden ten behoeve van de functionaliteiten over de verschillende afdelingen in combinatie met hun organisatorische rollen. De beste manieren om deze rollen tot stand te laten komen zijn via de bottum-up en by-example methode. Informatie vergaren over de rollen zal inhouden een uitdraai te maken van de Active Directory (AD) om deze vervolgens te sorteren. Na het sorteren zullen interviews plaatsvinden met de managers over wat de organisatorische rollen zijn. Indien dit geheel compleet is, zal een afweging gemaakt moeten worden welke rollen nu daadwerkelijk gecreëerd dienen te worden. Dit zal resulteren in een combinatie van de functionele en organisatorische rollen. Als laatste zullen de medewerkers gekoppeld worden aan de rollen die men behoort te hebben.

De voordelen van deze methode zijn dat in de huidige situatie alleen een verlaging op organisatorisch niveau plaats dient te vinden en er rollen tussen komen te zitten. Tevens is deze methode gemakkelijk uit te bereiden of te verkleinen. Voor deze methode is geen extra software of programmatuur benodigd.

De nadelen van deze methode zijn dat maar beperkte duidelijkheid wordt geboden, waardoor controle moeilijk word. Hierdoor is het systeem erg onderhevig aan wildgroei, omdat men niet duidelijk inzicht heeft in de rechten die aan de rollen zijn gekoppeld. Hierdoor kunnen dubbele rollen ontstaan. Ook de mogelijkheid dat men rollen heeft die niet gekoppeld mogen worden is aanwezig. Het onderhoud aan deze methode is hierdoor een tijdrovend geheel dat naar de toekomst toe alleen maar toeneemt. Door de gekozen methode blijft het met betrekking tot security dan een vraagstuk of dit door een medewerker kan gebeuren die de operatie als hoofdtaak en security als neven taak heeft. Ook de vraag of dit geheel risicodekkend is blijft bestaan.

***Voordelen***

* Makkelijk te implementeren.
* Gemakkelijk uitbreidbaar of te verkleinen
* Eenvoudige structuur.
* Geen extra programmatuur of software nodig.

***Nadelen***

* Beperkte duidelijkheid in de structuur.
* Niet gemakkelijk te controleren.
* Snel onderhevig aan wildgroei.
* Mogelijk dubbele rollen.
* Tijdrovend met betrekking tot onderhoud.
* Medewerker hoofdtaak operatie en neventaak security?
* Geheel risico dekkend?



## 4.3 Optie 3 - Limited Static Constrained RBAC

Het invoeren van de niveaus één, twee en drie (Limited Static Constrained RBAC) van het RBAC model. In figuur 4.3 is de template weergegeven van deze optie. Limited bij deze optie wil zeggen dat voor bepaalde functies is gekozen om deze niet te combineren, tenzij expliciete toestemming wordt gegeven. Deze toestemming zal van tijdelijke aard zijn of er hangt een geldigheidsduur aan vast die na het verlopen van de periode vernieuwd moet worden. Dit om te zorgen dat het beheersbaar blijft, niet verwaterd of wordt vergeten. Als regel zal worden gekozen voor het niet combineren van functies, tenzij strikt noodzakelijk. Het combineren van functies zal dus enkel gebeuren als uitzondering.

Aan de hand van de theorie is een template ontwikkeld, waarin al deze facetten terugkomen en die de risico's afdekken. De wijze van rol ontwikkeling zal bestaan uit een combinatie van de by-example en bottum-up methodes. Informatie vergaren over de rollen zal inhouden een uitdraai te maken van de Active Directory (AD) om deze vervolgens te sorteren. Na het sorteren zullen interviews plaatsvinden met de managers om inzicht te krijgen in de organisatorische rollen. Indien dit geheel compleet is, zal een afweging gemaakt moeten worden welke rollen nu daadwerkelijk gecreëerd dienen te worden. Aansluitend zal een afweging gemaakt dienen te worden welke functionaliteiten men wel en welke men niet mag combineren. Het uiteindelijke resultaat zal zijn dat combinaties van de functionele en organisatorische rollen gemaakt worden. Als laatste zullen de medewerkers gekoppeld worden aan de rollen die men behoort te hebben.

De voordelen van deze methode zijn dat in de huidige situatie verlaging op zowel organisatorisch als functioneel niveau plaats vindt met scheiding van functionaliteiten. Hierdoor ontstaat een duidelijke structuur. Door de duidelijkheid in de structuur is het ook gemakkelijker om deze rollen te onderhouden, beheren en controleren (audit). Tevens is het mogelijk om deze optie uit te bereiden of te verkleinen naar de wens van de organisatie. Voor deze methode is geen extra software of programmatuur benodigd.

De nadelen van deze methode zijn dat mogelijk teveel uitzonderingen op de regel blijven bestaan. Tevens door de omvang van deze methode en de mogelijke uitbereiding naar de onderliggende systemen is het wenselijk dat de werknemer die dit gaat onderhouden en beheren security als hoofdtaak heeft en niet de operatie. Door de gekozen methode blijft het met betrekking tot security dan ook een vraagstuk of dit door een medewerker kan gebeuren die de operatie als hoofdtaak en security als neven taak heeft. Ook de vraag of dit geheel risicodekkend is blijft bestaan.

***Voordelen:***

* Eenvoud waardoor het makkelijker te onderhouden en beheren is.
* Duidelijkheid in de structuur zowel organisatorisch als functioneel.
* Gemakkelijk uitbreidbaar of te verkleinen.
* Geen extra programmatuur of software nodig.
* Makkelijk te controleren (audit).

***Nadelen:***

* Teveel uitzonderingen op de regel?
* Medewerker hoofdtaak operatie en neventaak security?
* Geheel risico dekkend?



## 4.4 Optie 4 - Symmetric RBAC

Het invoeren van Symmetric RBAC. Deze optie is een pakket dat is ontwikkeld, waarbij de rollen en rechten met betrekking tot functionele en organisatorische rollen volledig geautomatiseerd worden toegekend.

Voordelen van deze methode zijn dat tot in detail van iedere medewerker gekeken kan worden wat benodigd is qua rechten. Ook de kans op fouten is kleiner, omdat het een geautomatiseerd systeem is en de rechten per medewerker worden toegekend.

Nadelen van deze methode zijn de kosten voor de ontwikkeling van het pakket evenals de kosten van invoering die hoog kunnen zijn. Ook de tijd die men kwijt is om het geheel te implementeren is erg veel en moeilijk vast te stellen.

***Voordelen:***

* Specifiek voor iedere medewerker.
* Geautomatiseerd systeem dus minder kans op fouten.

***Nadelen:***

* Maatwerk pakket (software) dus zeer hoog in kosten.
* Inrichting, ontwikkeling en specificatie erg langdurend proces.

## 4.5 Opties gewogen

Kostenefficiënt voor CMS wil zeggen dat het op een dusdanige wijze ingericht dient te worden dat dit geen extra kosten met zich meebrengt. Met extra kosten bedoelt men een investering in materiële zaken, zoals hardware en software. Naar aanleiding van de opties is het voor CMS niet aantrekkelijk om voor optie 4 te kiezen in verband met de hoge kosten die hiermee gemaakt worden. De opties 1 tot en met 3 bieden CMS de mogelijkheden om een aantal beveiligingsrisico's te minimaliseren zonder dat extra kosten gemaakt moeten worden.

De risico's minimaliseren is het speerpunt van dit project dat aansluit op de visie van Ciber. Risico's in kaart brengen is heel moeilijk met betrekking tot de schade uitgedrukt in geld en wat de daadwerkelijke consequenties zijn. De vraag van CMS is dus ook of de opties de risico's minimaliseren of niet. Als men de opties erbij pakt en daar naar kijkt is het voor optie 1 geen verandering van de huidige situatie en dekt het de risico's niet voldoende af. Voor de opties 2 tot en met 4 zijn de mogelijkheden om de risico's af te dekken aanzienlijk groter. Dit levert een verbetering van de huidige situatie, waardoor deze opties acceptabel zijn.

Door de invoering van RBAC is de vraag gerezen bij CMS of dit wel beheersbaar is. De beheersbaarheid is afhankelijk van de inrichting en het op een juiste wijze implementeren wat helderheid met betrekking tot de structuur met zich meebrengt. Ook zal CMS als geheel achter de invoering moeten staan en dit uitdragen richting het personeel en haar klanten. Als men kijkt naar optie 1 en 2 dan zijn deze te beperkt ten aanzien van de beheersbaarheid. De mogelijkheid bestaat nog steeds dat wildgroei ontstaat en dubbele rollen voorkomen, wat niet wenselijk is voor CMS. Voor de opties 3 en 4 zijn voldoende mogelijkheden om onderhoud te doen en de omgeving beheersbaar te houden.

CMS heeft als slogan "Client focused. Results driven". Deze toewijding is te zien bij het werk en de betrokkenheid van het personeel. De huidige kwaliteit van werken is hoog en om te zorgen dat de kwaliteit niet verloren gaat maar zelfs verhoogd wordt is het van belang dat de gekozen RBAC optie de controle middelen heeft om dit te bereiken. Opties 1 heeft minimale controle middelen en is dus te beperkt en te omslachtig om dit in stand te houden. De opties 2, 3 en 4 hebben meer controle middelen en zijn beter toepasbaar voor CMS.

Voor CMS is het tevens van belang dat de optie acceptabel is, waardoor meer draagkracht ontstaat. De draagkracht zal resulteren in aantoonbaar betere dienstverlening naar de klanten wat CMS sterker maakt. RBAC kan op veel manieren geïmplementeerd worden. In deze hoedanigheid bieden opties 1 en 2 geen duidelijke veranderingen van de huidige situatie. Opties 3 en 4 daarentegen brengen duidelijke veranderingen met zich mee op verschillende niveaus en dit zal uiteindelijk ook positief reflecteren richting de klanten.

Bovenstaande criteria zijn in tabel 1 weergegeven om inzichtelijk te maken welke optie het beste bij CMS past.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Eisen:** | **Optie 1** | **Optie 2** | **Optie 3** | **Optie 4** |
| Kostenefficiënt | v | v | v | x |
| Risico dekkend | x | v | v | v |
| Beheersbaar | x | x | v | v |
| Kwaliteitverhogend | x | v | v | v |
| Acceptabel binnen CMS | x | v | v | v |

Tabel 1.

Gericht op CMS en ook de afweging van de criteria gaat het advies uit naar optie 3. De optie raakt alle hoekstenen van RBAC en de optie past op dit moment, maar ook kijkend naar de toekomst, het beste bij CMS.

Bij de keuze voor optie 3 zijn nog een aantal randvoorwaarden van belang om de uiteindelijke implementatie met succes te kunnen afronden.

* Toewijding van het Management Team.
* Procedures helder beschrijven en borgen.
* Duidelijke communicatie richting de werknemers.
* Zo min mogelijk dubbelfuncties met betrekking tot security en de operatie.
* Plan voor verdere implementatie in de diverse systemen.

RBAC zal zowel procedureel als technisch geïmplementeerd worden en dit kan resulteren in weerstand, omdat het verandering met zich meebrengt. RBAC is een eigenschap van security en een onderdeel van het beveiligingsbeleid van CMS. Het is mogelijk om security als neventaak van een huidige functie te zien maar is niet wenselijk. De laatste jaren is men in de ICT dienstverlening meer en meer op het gebied van security aan het ontwikkelen en uitbereiden waardoor het tegenwoordig als een apart vakgebied kan worden beschouwt. Het is dan dus ook een aanbeveling om dit ook zo te gaan zien en indien dit mogelijk is te koppelen aan een functie.

# 5. Implementatie RBAC

De keuze van het Management Team (MT) om niveau 3 van het RBAC model te gebruiken met de daarbij behorende template, heeft geleid tot de start van de vergaderingen met de teamleads van de afdelingen Networking & Storage en Servers. De vergaderingen met de teamleads heeft als voornaamste doel het betrekken van de medewerkers en inzicht in het project te verschaffen. De gedachtegang die hiermee gecreëerd wordt is dat alle neuzen dezelfde kant op staan en dat de richting en het doel duidelijk wordt, waarnaar toegewerkt wordt. Tevens hebben de teamleads de mogelijkheid om te bepalen hoeveel niveaus aanwezig zijn binnen hun afdelingen en of de huidige opzet van de afdeling ideaal is of moet wijzigen.

## 5.1 Huidige situatie met rechten en rollen

De huidige situatie bij beide afdelingen is dusdanig ingericht dat geen onderscheid wordt gemaakt tussen de verschillende medewerkers. Tevens is het zo dat rechten zijn toegekend aan medewerkers en niet aan rollen of afdelingen. Dit is zo gegroeid uit noodzaak om de situatie werkbaar te houden. Om een gedegen uitgangspunt te hebben wat nodig is om RBAC in te voeren, is de Active Directory (AD) geschoond en terug gebracht naar een voor dit project werkbare situatie. Het is van belang dat RBAC wordt ingevoerd zonder dat de operatie gestoord wordt. Dit levert een extra dimensie op die inhoudt dat we niet een nieuwe omgeving kunnen maken maar dit bij de huidige omgeving moeten implementeren. Als laatste dient de omgeving geschoond te worden, zodat uiteindelijk alleen de rollen blijven bestaan.

Na het schonen dient de omgeving geëvalueerd te worden, omdat het toekennen van rechten in de huidige omgeving dusdanig omvangrijk is dat mogelijk teveel of te weinig rechten zijn toegekend aan een rol. Hierdoor ontstaan mogelijk ongewenste risico's.

De huidige situatie met betrekking tot rechten en rollen is weggezet in een schematische weergave om duidelijkheid te verschaffen en is weergegeven in figuur 5.1.



In figuur 5.1 kan men zien dat medewerkers rechten hebben maar ook de afdelingen en dat deze niet beperkt zijn tot hun afdeling. Hierdoor is het bijvoorbeeld mogelijk om als medewerker van de afdeling Networking & Storage om bepaalde handelingen uit te voeren op servers die niet gewenst is.

## 5.2 Naamgevingconventie voor rollen

Om de template goed te kunnen toepassen is het noodzakelijk om een naamgevingconventie te gebruiken die is gedefinieerd op een dusdanige wijze dat men hier in de toekomst ook profeit van heeft. Na onderzoek en gesprekken met verschillende teamleads en managers is gebleken dat RBAC mogelijk in de toekomst ook medewerkers van Ciber in ander landen zou kunnen betreffen. Tevens zijn er mogelijk ook 3rd party suppliers die toegang en rechten op de omgeving nodig hebben.

De naamgevingconventie die hieruit is ontstaan en goedgekeurd ziet er als volgt uit:

* NL = Country code;
* CMS = Business Line;
* SE = System Engineering;
* NET = Department;
* SENIOR = Function.

In de Active Directory (AD) wordt de rol dan als volgt weergegeven:

* NL-CMS SE-NET SENIOR.

De rollen kunnen nu op uniforme wijze worden benoemd en met de begeleidende documenten heeft men algeheel inzicht in de rollen.

## 5.3 Implementatie afdeling Networking & Storage

Uit de vergadering met de teamlead van de afdeling Networking & Storage is gebleken om voor de afdeling de twee disciplines te splitsen. Het idee van de teamlead om dit te doen is gebaseerd op de verschillende componenten en systemen in de onderliggende lagen waar men dagelijks mee werkt. Om een voorbeeld te geven: het was mogelijk om als medewerker van de deelafdeling Netwerken in te loggen op de verschillende Storage componenten. Ondanks dat de medewerkers dit niet doen en zich alleen bezig houden met hun eigen vakgebied heeft. De teamlead heeft de keuze gemaakt om de risico's te minimaliseren conform het gewenste beveiligingsbeleid en de rollen te splitsen.

De verschillende niveaus binnen Networking en Storage zijn gemaakt om aan te geven dat verschillen aanwezig zijn op het gebied van ervaring en functie. Verder is het de bedoeling om RBAC uiteindelijk door te voeren op de verschillende systemen. Een voorbeeld hiervan is het inrichten van RBAC conform de template op de netwerk componenten en in de Storage omgeving. Bij deze twee componenten wordt dus in overweging genomen om geïntegreerd met de Active Directory (AD) te functioneren. Bij beide componenten geeft dit mogelijk lastige of onwerkbare situaties dus men is heel voorzichtig met de uitrol.

Aansluitend op de template is in de AD de nieuwe situatie gecreëerd. De nieuwe situatie met rechten en rollen heeft nogal wat tijd gekost, omdat de operatie niet verstoord mocht worden. Het was noodzakelijk om een manier te vinden om de rechten zoals deze waren compleet te filteren en deze te koppelen aan de nieuwe rollen. De medewerkers zijn gekoppeld aan de rollen die men heeft gekregen. Op dit moment worden de rechten van de rollen opnieuw geëvalueerd of dit compleet conform het gewenste resultaat is. Deze evaluatie neemt veel tijd in beslag en is helaas op geen andere mogelijkheid te doen, omdat het een bestaande omgeving betreft en het werk gewoon door gaat. Het idee is wel dat men in zover mogelijk het principe van "Least Privilege" toepast. Dit om er zeker van te zijn dat de risico's geminimaliseerd zijn en dat de uitzonderingen gedocumenteerd worden.

In figuur 5.2 is de ingevulde template weergegeven van de gewenste situatie met rollen voor de afdeling Networking & Storage.



## 5.4 Implementatie afdeling Servers

Uit de vergadering met de teamlead van de afdeling servers is gebleken dat de functieprofielen van de afdeling maar ook het technische verantwoording niet geheel duidelijk is en dat de rechten die men op dit moment heeft moeilijk zijn te schalen naar een niveau of rol. Toch is de template toegepast en is er invulling gegeven aan het veiligheidsbeleid. De rechten daarentegen die gekoppeld dienen te worden aan de rollen worden op dit moment geëvalueerd en er wordt gekeken of er een duidelijke scheiding aangebracht kan worden tussen de niveaus.

In figuur 5.3 is de ingevulde template weergegeven met de huidige stand van zaken met betrekking tot de afdeling servers.



# 6. Advies implementatie overige afdelingen

Het advies dat in dit hoofdstuk wordt gegeven is een advies wat passend bij de huidige situatie van CMS. CMS is op dit moment bezig om een aantal grote klanten binnen te halen waardoor de focus primair op de klant gericht is.

De overige afdelingen zijn in de onderliggende lagen sterk vertegenwoordigd, maar dat neemt niet weg dat de inrichting van RBAC op de buitenste laag al dient te worden geïmplementeerd. De gevolgde aanpak kan gewoon worden doorgezet en deze wordt verderop beschreven.

## 6.1 Aanpak implementatie per afdeling

De aanpak die hier is beschreven geeft de teamlead de ruimte en mogelijkheid om de afdeling conform de template weg te zetten. De bedoeling is dat de teamlead de verantwoording draagt over de eventuele niveaus in zijn afdeling, omdat deze tenslotte eindverantwoordelijk is voor de afdeling. De teamlead deelt de medewerkers in aan de hand van het functieprofiel en de ervaring van de medewerkers. De teamlead is hier vrij in en wordt niet belemmerd door organisatorische rollen. Het ideaal beeld is natuurlijk dat de teamlead op zowel ervaringsniveau als organisatorisch de juiste invulling hieraan geeft.

In samenspraak met de teamlead worden eventuele beveiligingsrisico's besproken en gekeken of tot structurele oplossingen gekomen kan worden. Tevens wordt in de onderliggende lagen gekeken of het mogelijk is om de template toe te passen en of dit reëel is voor de desbetreffende afdeling. Het is namelijk niet de bedoeling dat RBAC op de onderliggende lagen wordt ingevoerd om het beveiligingsbeleid te implementeren. Het is de bedoeling om de risico's te minimaliseren en het moet een werkbare situatie blijven.

Nadat invulling is gegeven aan de template die in samenspraak met desbetreffende teamlead is gemaakt, wordt met een specialist van de afdeling Servers een afspraak gemaakt om te bepalen wat de beste methode is om deze afdeling conform de template in te richten. De inrichting van de rollen kan inhouden dat een testperiode plaatsvindt met maar één medewerker in de nieuwe structuur. Dit om te beoordelen of alle rechten gekoppeld aan de rollen juist zijn en of de RBAC inrichting een werkbare situatie is. De operatie gaat namelijk gewoon door en door deze test periode is de kans op verstoringen minimaal. Aansluitend aan de testperiode, en met goedkeuring van de teamlead, wordt de afdeling in zijn geheel naar de nieuwe situatie overgezet.

Wanneer de gehele afdeling is omgezet naar de nieuwe situatie kan de oude omgeving opgeruimd worden en vindt tegelijkertijd de evaluatie van de rollen plaats. De evaluatie van de rollen is bedoeld om te beoordelen of het principe van "least privilege" is toegepast. Indien nodig worden correcties op de rollen doorgevoerd in overeenstemming met de teamlead.

Tenslotte dient de nieuwe situatie gedocumenteerd te worden en opgenomen in de bedrijfsprocessen zodat dit de nieuwe standaard wordt. Door de documentatie is het tevens mogelijk om de controle middelen voor auditing op een correcte wijze op te zetten. Met documenteren van de nieuwe situatie is het namelijk mogelijk dat sommige rechten die men eerder wel had binnen de afdeling nu niet meer aanwezig zijn. Een mogelijk voorbeeld zou kunnen zijn dat men bij de afdeling Databases rechten had op een server om services te herstarten. Conform Information Technology Infrastructure Library (ITIL) en ook het verantwoordingsbereik van de afdeling zou dit niet mogelijk moeten zijn. De mogelijkheid en de verantwoordelijkheid om een service te herstarten hoort thuis bij de afdeling Servers. De afdeling Databases zou alleen maar toegang behoren te hebben tot de databases en al hun werkzaamheden op die laag moeten kunnen verrichten. Mocht het nodig zijn om een service te herstarten dan zou dit door de afdeling Servers moeten worden uitgevoerd.

Een voordeel van deze methode van implementatie is dat uiteindelijk geen onbekende factoren en verantwoordelijkheden meer aanwezig zijn waar niemand verantwoordelijk voor is. De bedoeling is dus tweeledig en deze zijn het inzichtelijk maken en documenteren van de verantwoordelijkheden en conform het beveiligingsbeleid de risico's minimaliseren middels RBAC.

# 7. Conclusies en aanbevelingen

In dit hoofdstuk worden de conclusies en aanbevelingen besproken. Als eerste volgen de conclusies van het RBAC project en aansluitend de aanbevelingen.

## 7.1 Conclusies

RBAC is een lopend project binnen CMS om deels invulling te geven aan het beveiligingsbeleid. De beschikbaarheid, integriteit en vertrouwelijkheid van data en informatiesystemen zijn de speerpunten van klanten als het gaat om uitbesteding van de ICT in zijn geheel of een component daarvan. Het RBAC project is voor zowel de klant als voor CMS een belangrijk speerpunt om te realiseren. De reflectie richting de klant van de hoogte en diepgang van de geïmplementeerde maatregelen op het gebied van informatiebeveiliging, maar ook de documentatie ervan inclusief de bedrijfsprocessen, geeft de klant een duidelijk beeld hoe met informatie van de klant omgegaan wordt.

Men is inmiddels binnen de verschillende afdelingen aan het kijken voor een mogelijkheid om RBAC in de onderliggende lagen, zoals op databases en applicaties, te implementeren. Men komt dus ook gevraagd en ongevraagd voor advies over bepaalde elementen en mogelijkheden ten behoeve van RBAC. Dit heeft als resultaat dat de toewijding van CMS ver boven verwachting is omdat, men niet alleen bezig is met de operatie en toekomstige klanten maar ook de toekomst van CMS. De visie die hiermee is gecreëerd is een duidelijke en heldere visie die bij iedere medewerker bekend is en geeft een hoge mate van professionaliteit weer.

Gericht op het project is het van belang dat de toewijding van het MT blijft bestaan en dat regelmatig om status updates gevraagd wordt. Tevens zal vanuit het security team regelmatig gekeken moeten worden of de vooruitgang nog steeds conform het beveiligingsbeleid is en of de elementen op correcte wijze gedocumenteerd zijn. Dit heeft als doel de juist controle middelen en methoden in plaats te brengen voor audits.

## 7.2 Aanbevelingen

De aanbeveling blijft bestaan dat eerst de buitenste laag gereed dient te zijn voordat, men gaat kijken naar de onderliggende lagen. Deze structuur is van belang, zodat men niet RBAC gaat toepassen voor RBAC, maar voor de systemen om op deze wijze invulling aan het beveiligingsbeleid te geven en de risico's afdekken. Tevens is de kans op onnodig veel rollen en het kwijtraken van een duidelijke structuur tot een minimum terug gebracht. Dit neemt niet weg dat constant geëvalueerd moet worden of dit de werkbaarheid in gedrang brengt.

De betrokkenheid van de teamleads is een belangrijke spil in dit project. Het is dan ook een aanbeveling, omdat het de kans van slagen vergroot, maar ook vanwege de expertise die men met zich meebrengt. Deze betrokkenheid creëert men door vanaf het begin duidelijk te communiceren met de teamleads en deze ook de verantwoording te geven die men behoort te krijgen.

# 8. Evaluatie

Na het accepteren van de afstudeeropdracht ben ik mezelf gaan verdiepen in RBAC waar ik aanvankelijk niet zo heel bekend mee was. Na het uitzoeken van verschillende theorieën en "best practices" had ik globaal een indicatie wat van mij werd verwacht. Dit is ook de insteek die mij bij de opleiding is geleerd.

De start van mijn afstudeeropdracht is, naar mijn mening, nogal traag verlopen. Dit kwam vooral, omdat ik de kennis van het bedrijf en de omgeving gewoonweg niet had. Tevens heeft het mijn begeleiders tijd gekost om mij de juiste weg te wijzen. De reden dat dit naar mijn idee langer heeft geduurd is dat ik uit een andere omgeving en bedrijfscultuur kom waar alles op een andere manier werkt. Niet geheel onbelangrijk is dat het beleid uit de omgeving waar ik vandaan kom al is ontwikkeld en ik daar voor een gedeelte invulling daaraan geef, terwijl ik hier onderdeel uitmaak van het ontwikkelen van het beleid dat uitgedragen dient te worden. Dit heeft mij dus geleerd om een ander manier van denken aan te nemen.

Nadat mijn begeleiders mij op het juist pad hebben gezet, ben ik begonnen aan de theorie van RBAC. De theorie is in deze gekozen door het bedrijf en is een van de vele die men zou kunnen toepassen. De moeilijkheidsgraad zat hem voor mij in een generieke template te creëren die gericht is op de toekomst. Door een aantal gesprekken met zowel Jan Weerts mijn begeleider en de Security Officer Ben Beens ben ik op het juiste idee uitgekomen. Dat idee heb ik vervolgens verder uitgewerkt. Dit heeft geresulteerd in een template die generiek toepasbaar is en gericht op de toekomst. De template is in mijn ogen de voorbereiding die benodigd is om RBAC goed te implementeren.

Nadat de beslissing gemaakt was door het MT werd het tijd voor de volgende stap, namelijk de implementatie. De implementatie heeft meer vertraging opgelopen dan ik initieel gehoopt had. Dat heeft vooral te maken met de bedrijfscultuur en het motto van Ciber. De klant komt altijd van rechts voor de Ciberianen. Ik sta 100% achter dat motto. Het gaat tenslotte om mogelijk nieuwe klanten en een hogere omzet. Ondanks dat RBAC maar voor 1 van de 2 afdelingen compleet is geïmplementeerd, heeft dat mijn leercurve en technische expertise niet belemmerd. Ik ben zelfs van mening dat dit heeft geresulteerd in een betere bewustwording over hoe belangrijk het RBAC project is voor CMS om goed uit te voeren.

Het advies over de invoering op de overige afdelingen is vooral gericht op de volgende stap. Het is hierbij essentieel om de teamleads, maar ook de medewerkers, het nut en belang van het project te laten inzien. Ondanks dat de teamleads niet altijd evenveel tijd voor mij beschikbaar hadden, hebben zij toch een zeer waardevolle bijdrage gegeven aan het RBAC project. Dit heeft mij meer inzicht gegeven in de verschillende afdelingen en hun werkwijzen.

Het management is zich bewust dat de invoering van RBAC doorgang moet vinden en het is dus van belang om als projectleider met duidelijke resultaten te komen. Dit is mij geleerd dat je als projectleider met duidelijke resultaten een hoop kunt bereiken. Het belangrijkste echter is toch dat je genoegen moet nemen met bepaalde situaties zoals nieuwe klanten of iets dergelijks. Het gaat uiteindelijk om een ding en dat is omzet.

# Literatuur

Fijneman, R., Roos Lindgreen, E., Hang Ho, K. (2011). *IT-auditing en de praktijk.* 2e druk. Academic Service, SDU Uitgevers BV. ISBN 978-90-395-2627-9

Hogewoning, K., Lith G., Kraan van der, M.G.M., Verburg A.J. & anderen (2007). *Internet security. De beveiliging van aan internet gekoppelde netwerken.* 1e druk. Vanveen informatica BV. ISBN 978-90-71501-16-6

Verscheidene auteurs (2010). *Information Security Foundation.* 3e druk. E3 ICT.

ISBN 90-76939-71-3

# Geraadpleegde internetsites

*Bedrijfsinformatie:*

[http://www.ciber.nl/](http://www.ciber.nl/%20) (mei 2012)

*Verdieping informatiebeveiliging:*

<http://nl.wikipedia.org/wiki/Informatiebeveiliging> (april 2012)

*Verdieping theorie RBAC:*

[http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf](http://csrc.nist.gov/rbac/sandhu-ferraiolo-kuhn-00.pdf%20) (2000)

<http://csrc.nist.gov/groups/SNS/rbac/> (mei 2009)

[http://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC](http://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC%20) (april 2012)

*Verdieping role-mining:*

<http://searchsecurity.techtarget.com/definition/role-mining> (maart 2008)

*Nederlandse taal:*

<http://synoniemen.net/> (mei 2012)Afkortingenlijst

AD = Active Directory (windows)

BL = Business Line

CMS = Ciber Managed Services

DSD = Dynamic Separation of Duty

ICT = Informatie en Communicatie Technologie

ITIL = Information Technology Infrastructure Library

IT = Informatie Technologie

MS = Management en Security

MT = Management Team

NIST = National Institute for Standards and Technology

PID = Project Initiation Document

PVA = Plan van aanpak

RBAC = Role Based Access Control

SOD = Segregation of Duties

SSD = Static Segregation of Duty

# Bijlage A Plan van aanpak

Plan Van Aanpak

RBAC, onderzoek en implementatie binnen Ciber Managed Services.

Datum: 16-2-2012

****

|  |  |  |  |
| --- | --- | --- | --- |
| **Opdrachtgever:** | | | |
|  | **Achternaam:** | **Voornaam:** | **E-mail adres:** |
|  | Toorenburg, van | Leon | Leon.van.Toorenburg@Ciber.nl |
| **Opdrachtnemer:** | | | |
| **Student Nummer:** | **Achternaam:** | **Voornaam:** | **E-mail Adres:** |
| 2158962 | Vaes | Patrick | car\_casstro@hotmail.com |
|  |  |  |  |

Auteur: P.H.M. Vaes Versie: 1.0 DefinitiefInhoudsopgave

[1. Management samenvatting 3](#_Toc325292497)

[2. Introductie 4](#_Toc325292498)

[a. Aanleiding 5](#_Toc325292499)

[b. Goedkeuring en eventuele bijstelling 5](#_Toc325292500)

[c. Toelichting op de opbouw van het plan 6](#_Toc325292501)

[3. Projectopdracht 6](#_Toc325292502)

[a. Projectomgeving 6](#_Toc325292503)

[b. Doelstelling project 6](#_Toc325292504)

[c. Opdrachtformulering 8](#_Toc325292505)

[d. Op te leveren producten en diensten 8](#_Toc325292506)

[e. Eisen en beperkingen 9](#_Toc325292507)

[f. Cruciale succesfactoren 9](#_Toc325292508)

[4. Aanpak 10](#_Toc325292509)

[a. Adviesrapport methode en technieken 10](#_Toc325292510)

[b. Template aan de hand van de gekozen methode of technieken 10](#_Toc325292511)

[c. Test en implementatie plan 10](#_Toc325292512)

[d. Adviesrapport over de mogelijke invoering overige afdelingen 10](#_Toc325292513)

[5. Projectinrichting en voorwaarden 11](#_Toc325292514)

[a. Projectinrichting 11](#_Toc325292515)

[b. Voorwaarden aan opdrachtnemer 11](#_Toc325292516)

[6. Plannen 12](#_Toc325292517)

[a. Normen en aannames 12](#_Toc325292518)

[b. Activiteiten, Producten en Mijlpalen 12](#_Toc325292519)

[c. Resourceplan 13](#_Toc325292520)

[d. Risicoanalyse](#_Toc325292521) 13

[e. Kosten-batenanalyse 18](#_Toc325292522)

[7. Kwaliteitsborging 19](#_Toc325292523)

[a. Productkwaliteit 19](#_Toc325292524)

[b. Proceskwaliteit 19](#_Toc325292525)

[8. Bijlagen 19](#_Toc325292526)

# 

# Management samenvatting

Als ICT dienstverlener heeft men te maken met toegang tot verschillende ICT omgevingen zowel bij klanten als intern. Om ervoor te zorgen dat de risico's geminimaliseerd zijn gebeurd dit doormiddel van het beperken van toegang en het toekennen van rechten via een standaard methode. De methode die hieruit is ontstaan noemt men Role Based Access Control (RBAC). Deze methode is op alle systemen toepasbaar alleen in hoeverre is per systeem afhankelijk.

Om een juiste uitvoering te geven aan de visie van het beveiligingsbeleid wordt in dit plan van aanpak het volgende besproken.

Het onderzoeken en invoeren van RBAC binnen Ciber Managed Services (CMS) omvat de volgende hoofdpunten:

* Onderzoeken welke methoden of technieken het beste bij Ciber aansluiten.
* Template maken van de methode of techniek die het beste past.
* Testen en invoeren in de operationele omgeving op de afdelingen Networking en Storage en Servers.
* Adviesrapport schrijven over de invoering op de overige afdelingen.

Beslispunten in deze zijn:

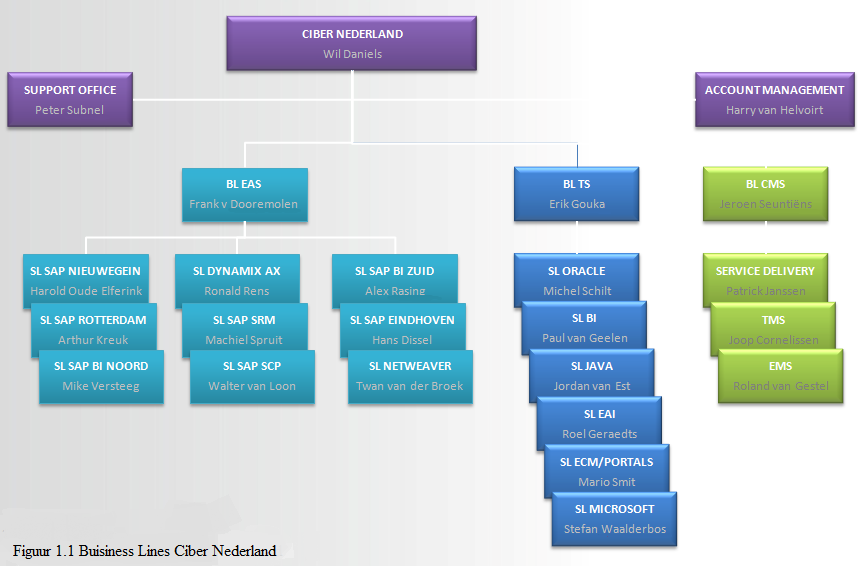
* De methode of techniek die het beste bij Ciber past.
* Het adviesrapport als basis voor het wel of niet invoeren op de overige afdelingen.

De informatie van deze samenvatting en de overige informatie die is verzameld is verder uitgewerkt en onderbouwt in dit plan van aanpak.

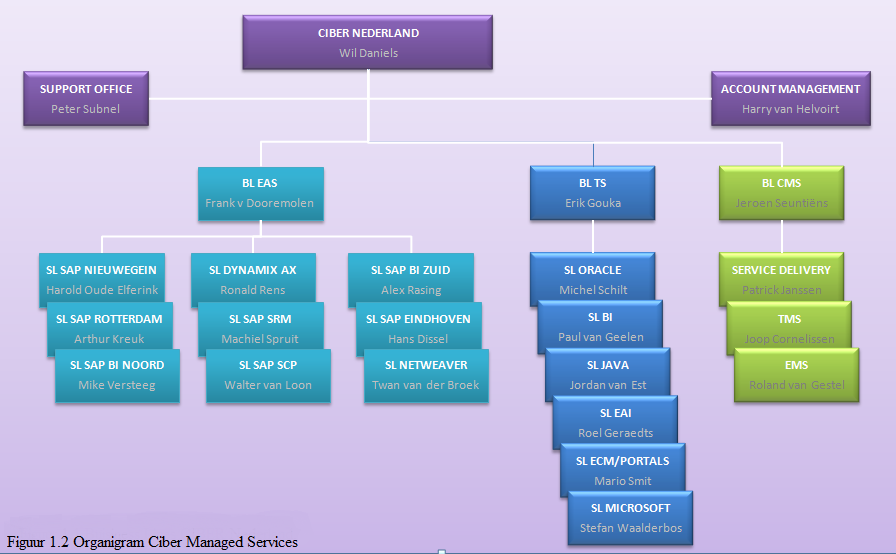
# Introductie

Ciber Incorporated is een full-service ICT dienstverlener ontstaan in 1974 met omzet van ongeveer 1,2 miljard USD in 2011 en beursgenoteerd op de New York Stock Exchange. Ciber Incorporated is een Gartner Tier 1 ICT dienstverlener met meer dan 9000 medewerkers verdeeld over 72 kantoren in 19 verschillende landen. Ciber Incorporated heeft de dienstverlening in zowel Onshore, Offshore als Nearshore.

Ciber Nederland is ontstaan in 1996 met een omzet van ongeveer 100 miljoen Euro in 2011. Ciber Nederland heeft ongeveer 525 medewerkers verdeeld over 5 kantoren. Ciber Nederland heeft de dienstverlening in zowel Offshore als Nearshore en is "preferred supplier" van een groot aantal Nederlandse multinationals. Ciber Nederland is onderverdeeld in een aantal Business Lines zoals weergegeven in figuur 1.



De Ciber Managed Services tak bedient haar klanten door de ICT dienstverlening over te nemen van de klant om zo de ICT systemen voor de klant te beheren. Tevens zijn alle specialiteiten die in de andere business lines vertegenwoordigd zijn ook aanwezig in de Ciber Managed Services tak. Een organigram van de Ciber Managed Services tak is in figuur 2 weergegeven.



## Aanleiding

Door de groei van Ciber Managed Services en de focus op internationalisering is de behoefte ontstaan om de informatie beveiliging van de dienstverlening beter te borgen en te garanderen. Naast lopende initiatieven heeft Ciber Managed Services ook de behoefte om op autorisatie niveau vanuit een centrale visie te gaan werken.

## Goedkeuring en eventuele bijstelling

Dag 16 februari 2012 wordt het concept plan van aanpak besproken. Naar aanleiding daarvan zal het plan op punten worden bij-, danwel uitgewerkt.

Naast de projectleider (Patrick Vaes) zijn er een aantal andere belanghebbenden te benoemen die een oordeel over (een deel van) het plan kunnen / moeten geven.

Lead Consultant Networking & Storage - Jan Weerts zal vanuit zijn rol als teamlead Networking & Storage en als mijn stagebegeleider een sturende rol hebben.

Security Officer - Ben Beens is verantwoordelijk voor het beveiligingsbeleid van Ciber Managed Services en zal mij begeleiden over de procedurele aanpak van het project.

Compliance Officer - Joep Smets zal mij begeleiden vanuit zijn rol als Compliance Officer en ondersteund bij vraagstukken over wet en regelgeving ten aanzien van de klanten die Ciber Managed Services bediend.

De voortgang en bijstellingen op het plan worden vastgesteld middels de voortgangsrapportage. Nadat voorgestelde wijzigingen zijn goedgekeurd is het plan van aanpak bijgesteld. Het actuele plan van aanpak wordt op deze wijze gevormd door het oorspronkelijke plan van aanpak en de voortgangsrapportages.

## Toelichting op de opbouw van het plan

De opbouw van dit plan is dat het op een gestructureerde en duidelijk afgebakende wijze wordt ingericht met de focus op een projectmanager die er fulltime mee bezig kan gaan. Dit om ervoor te zorgen dat er een zo goed mogelijk resultaat te bereiken.

# Projectopdracht

## Projectomgeving

Wat is het beschouwingsgebied?  
 De omgeving waarin dit project zich afspeelt is Ciber Managed Services en dan specifiek voor de afdelingen Netwerken & Storage en Servers. De afdelingen samen bestaat in het totaal uit 24 personen die zich bezig houden met de derde en vierde lijn ondersteuning voor de lopende operatie. Tevens doet men de planning, inrichting en gereedstelling van nieuwe projecten.

### Wat is de behoefte?

Role Based Access Control conform het NIST RBAC model invoeren binnen Ciber Managed Services. Om het project beheersbaar te houden is de scope geldig voor de afdelingen Networking & Storage en Servers.

### Waaruit is deze behoefte ontstaan?

De klant wil zekerheid van een afgenomen dienst. Om deze te bieden kijkend naar de visie van Ciber Managed Services is er gekozen voor Role Based Access Control conform het NIST RBAC model te implementeren binnen Ciber Managed Services.

## Doelstelling project

Doormiddel van een generieke aanpak, solide beveiligingsbeleid en de NIST RBAC methode wil men de klant zekerheid van een afgenomen dienst garanderen. Om dit te realiseren heeft men een gedegen basis nodig waaruit men kan werken.

### Waarom heeft de opdrachtgever het resultaat nodig en wat moet er worden bereikt?

Er wordt uitvoer gegeven aan de visie en tevens worden de risico's voor klanten en Ciber Managed Services verminderd. In deze hoedanigheid is er gekozen voor een generieke aanpak op alle niveaus en alle systemen. Het streven is kwaliteit die reflecteert richting de dienstverlening naar de klant.

### Doelstellingen:

* + 1. Het ontwerpen en onderzoeken van de mogelijkheden van Role Based Access Control afgeleid van het NIST RBAC model binnen Ciber Managed Services. Dit dient in eerste instantie te gebeuren op de afdelingen Networking & Storage en Servers. Dit dient op een correct wijze geplant en voorbereid te worden met als realisatiedatum 09-03-2012.
    2. Het beschrijven en borgen van de generieke aanpak binnen Ciber Managed Services waarmee RBAC geïmplementeerd kan worden. Hier dient uitvoering aan gegeven te worden op de afdelingen Networking & Storage en Servers met als realisatiedatum 30-03-2012.
    3. Het uitzoeken van de mogelijke technische oplossingen, waarop RBAC op een kostefficiënte manier op de afdelingen Networking & Storage en Servers kan worden geïmplementeerd. Hier dient een correcte uitvoering aan gegeven te worden zonder dat het de operationele doorgang verstoord met als realisatiedatum 04-05-2012.

### Resultaten:

1. Adviesrapport met de mogelijkheden voor Ciber Managed Services.
2. Een ontwikkelde methode of techniek die men kan toepassen binnen Ciber Managed Services.
3. Invoering van RBAC in de live omgeving.

## Opdrachtformulering

### Wat is de projectopdracht?

Het onderzoeken, ontwerpen, beschrijven en implementeren van RBAC op de afdelingen Networking & Storage en Servers binnen Ciber Managed Services.

Waarover gaat het project procesmatig (afbakening)?

Het uitzoeken van de mogelijkheden voor RBAC binnen de afdelingen Networking & Storage en Servers van Ciber Managed Services. Als leidraad zal de NIST RBAC Methode worden gehanteerd en daaruit vloeiend zal een manier gekozen worden die het beste kan worden geïmplementeerd binnen de operatie van Ciber Managed Services op de eerder genoemde afdelingen. Tevens wordt er een Template gecreëerd die men mogelijk kan toepassen binnen alle afdelingen van Ciber Managed Services.

Het project in deze heeft zowel een resultaat- als inspanningsverplichting. Resultaatsverplichtingen in deze zijn de ontwikkelde methode, template en de invoering hiervan met daaraan gekoppeld de gereedstelling. De inspanningsverplichting is het adviesrapport waaruit zal blijken of het gewenste doel te bereiken is.

## Op te leveren producten en diensten

Wat is het resultaat van het project?

Het resultaat van het project moet zijn dat de informatiebeveiliging van de dienstverlening geborgd en gegarandeerd is.

### Te leveren producten en diensten:

* Adviesrapport methode en technieken.
* Template aan de hand van de gekozen methode of techniek.
* Test en implementatie plan.
* Adviesrapport over de invoering op de overige afdelingen.

## Eisen en beperkingen

Er zijn een aantal eisen en beperkingen en deze staan hieronder weergegeven.

### Eisen:

* Uitvoer geven aan de visie en tevens de risico's voor klanten en Ciber Managed Services zoveel mogelijk te verminderen.
* Kwaliteit verhogen richting de dienstverlening naar de klant.
* Kosten efficiënt invulling geven aan de invoer van Role Based Access Control.

### Beperkingen:

* Operationele doorgang mag niet worden verstoord.
* Hier dient op een zo kost efficiënte manier invulling aan te worden gegeven.

## Cruciale succesfactoren

|  |  |
| --- | --- |
| Het Project: | |
|  | Duidelijk afgebakend begin en einde |
|  | Gestructureerde werkwijze en communicatie |
|  | Beperking van financiële en personele middelen |
|  | Het tijdig informeren van de verandering van werkwijze |

|  |  |  |
| --- | --- | --- |
| De Projectmanager: | | |
|  | | Patrick Vaes |
| De organisatie in deze de stuurgroep: | | | |
|  | Jan Weerts - Senior Consultant / Stagebegeleider | | |
|  | Ben Beens - Security Officer | | |
|  | Joep Smets - Compliance Officer | | |

# Aanpak

In dit hoofdstuk wordt de aanpak, de realisatie van de te leveren producten en diensten besproken. De indelingen hiervan is gemaakt op de te leveren dienst of product.

## Adviesrapport methode en technieken

Het adviesrapport methode en technieken zal worden samengesteld aan de hand van de theorie. De theorie is conform het document: "The NIST Model for Role-Based Access Control: Towards a Unified Standard" geschreven door de heren Ravi Sandhu, David Ferraiolo en Richard Kuhn uit het jaar 2000.

## Template aan de hand van de gekozen methode of technieken

Naar aanleiding van het advies rapport en de gewenste methode of technieken zal een keuze gemaakt worden wat het beste bij Ciber Managed Services past. Er zal een template ontwikkeld worden die het geheel inzichtelijk maakt en mogelijk zo uitgerold kan worden.

## Test en implementatie plan

Als de template is goedgekeurd dan is er een basis die kan worden gebruikt binnen Ciber Managed Services en voor dit project de afdelingen Networking & Storage en Servers. Hiervoor zal een test en implementatie plan geschreven worden met als speerpunt dat de operationele doorgang niet verstoord mag worden.

## Adviesrapport over de mogelijke invoering overige afdelingen

Het advies rapport over de mogelijke invoering bij overige afdelingen zal grotendeels bestaan uit een advies met de mogelijkheden en impact op de overige afdelingen.

# Projectinrichting en voorwaarden

## Projectinrichting

Bij projectinrichting wordt inzichtelijk gemaakt hoe de organisatie van het project er uit ziet om de opdracht uit te kunnen voeren volgens de voorgestelde aanpak. Deze is hieronder in een schematische weergave weergegeven.



## Voorwaarden aan opdrachtnemer

De voorwaarden die zijn gesteld zijn:

* Uitvoer geven aan de visie en tevens de risico's voor klanten en Ciber Managed Services zoveel mogelijk te verminderen.
* Kwaliteit verhogen richting de dienstverlening naar de klant.
* Hier dient op een zo kost efficiënte manier invulling aan te worden gegeven.
* Operationele doorgang mag niet worden verstoord.

# Plannen

## Normen en aannames

De norm en aanname die is gedaan is dat het inrichten van RBAC binnen Ciber Managed Services op een dusdanige wijze plaatsvindt dat het de risico's verminderd en past binnen de huidige situatie.

## Activiteiten, Producten en Mijlpalen

De activiteiten, producten en mijlpalen van dit project zijn weggezet in tijd en ruimte conform het onderstaande schema.

|  |  |  |  |
| --- | --- | --- | --- |
| **Activiteiten:** | **Datum:** | **Hoe:** | **Opmerkingen:** |
| Voortgangsrapportage met de Security Officer. | 17-2-12 | Bespreking. | - |
| Inleveren PvA en communicatieplan i.o.m. begeleidend docent. | 24-2-12 | Via mail en hardcopy. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 2-3-12 | Bespreking. | - |
| Adviesrapport methode en technieken. | 9-3-12 | Via mail en hardcopy. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 16-3-12 | Bespreking. | - |
| Voortgangsrapportage met de Security Officer. | 30-3-12 | Bespreking. | - |
| Template aan de hand van de gekozen methode of techniek | 30-3-12 | Via mail en hardcopy. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 13-4-12 | Bespreking. | - |
| Test en implementatie plan. | 20-4-12 | Via mail en harcopy. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 27-4-12 | Bespreking. | - |
| Adviesrapport over de invoering op de overige afdelingen. | 4-5-12 | Via mail en hardcopy. | Gereed. |

## Resourceplan

Het resourceplan is in deze volledig gericht op de personele inzet. De middelen zijn al aanwezig en worden in deze niet meegenomen.

|  |  |  |
| --- | --- | --- |
| **Opdrachtgever:** | **Functie & Niveau:** | **Wanneer en Hoe:** |
| Leon van Toorenburg | Team leader Managed Services Infrastructure Teams | when needed |
| **Stuurgroep:** | | |
| Jan Weerts | Lead Consultant Networking & Storage | part time |
| Ben Beens | Security Officer | part time |
| Joep Smets | Compliance Officer | part time |
| **Project leider:** | | |
| Patrick Vaes | Project leider | full time |
| **Overige:** | | |
| Afdeling SE-S | Leden van de afdeling | when needed |
| Afdeling SE-NS | Leden van de afdeling | when needed |
| Overige Afdelingen | Leden van de afdeling | when needed |

## Risicoanalyse

Er zijn twee manieren om een risicoanalyse uit te voeren en deze zijn :

* kwantitatief.
* kwalitatief.

De keuze van het type risicoanalyse is gevallen op kwalitatief omdat de risico's voor dit project geen directe waarde uitgedrukt in geld met zich meebrengen.

### Doel:

Het doel van deze risicoanalyse is het in kaart brengen van de risico's die bij dit project kunnen voorkomen. Deze risico's kunnen het beste geïdentificeerd worden met meerdere personen om zo tot het beste resultaat te komen. De geïdentificeerde risico's zijn hieronder weegegeven.

### Geïdentificeerde risico's:

1. ***Operationele doorgang:***
   1. Ingezet als operationeel medewerker.
   2. Medewerkers in de operatie hebben geen tijd.
   3. Geen beschikking over Ontwikkeling, Test en Acceptatie (OTA) straat.
2. ***Acceptatie werkvloer:***
   1. Management geeft geen akkoord.
   2. Management geeft geen draagkracht.
   3. Geen acceptatie vanaf de werkvloer.
3. ***Scope:***
   1. Opdrachtformulering is te uitgebreid.
   2. Oplossing is te globaal.
4. ***Tijd:***
   1. Niet voldoende tijd.
5. ***Inzetbaarheid projectleider:***
   1. Ziekte.

### Impact en Kans definitie:

De impact heeft betrekking tot het slagen van het project en is gedefinieerd in drie elementen zijnde laag, middel en hoog.

* *Impact laag*: Wil zeggen dat het mogelijk kan zijn dat het project enige vertraging kan oplopen.
* *Impact middel*: Wil zeggen dat er directe vertraging gaat optreden voor het project.
* *Impact hoog*: Wil zeggen dat hier meteen op gehandeld dient te worden want het project loopt in direct gevaar.

De kans heeft betrekking tot het volume van optreden. Dit wil zeggen dat het een of meerdere keren kan optreden.

* *Kans laag*: Wil zeggen dat het een enkele maal of niet voorkomt.
* *Kans middel*: Wil zeggen dat het een aantal maal kan voorkomen.
* *Kans hoog*: Wil zeggen dat het vaak kan voorkomen.

In het onderstaande schema zijn de hoofdrisico's met daaruit afgeleide subrisico's opgenomen en deze geïdentificeerd met de kans en impact.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hoofd Risico** | | **Sub Risico** | **Kans** | **Impact** |
| **1** | ***operationele doorgang*** |  |  |  |
| **1a** |  | Ingezet als operationeel medewerker. | ***laag*** | ***hoog*** |
| **1b** |  | Medewerkers in de operatie hebben geen tijd. | ***middel*** | ***middel*** |
| **1c** |  | Geen beschikking over OTA straat. | ***hoog*** | ***middel*** |
| **2** | ***acceptatie werkvloer*** |  |  |  |
| **2a** |  | Management geeft geen akkoord. | ***laag*** | ***hoog*** |
| **2b** |  | Management geeft geen draagkracht. | ***laag*** | ***hoog*** |
| **2c** |  | Geen acceptatie vanaf de werkvloer. | ***laag*** | ***middel*** |
| **3** | ***scope (te groot)*** |  |  |  |
| **3a** |  | Opdrachtforumlering is te uitgebreid. | ***laag*** | ***middel*** |
| **3b** |  | Oplossing is te globaal. | ***laag*** | ***middel*** |
| **4** | ***tijd (project en andere activiteiten)*** |  |  |  |
| **4a** |  | Niet voldoende tijd. | ***laag*** | ***hoog*** |
| **5** | ***inzetbaarheid projectleider*** |  |  |  |
| **5a** |  | Absentie door ziekte of andere omstandigheden. | ***laag*** | ***hoog*** |

### Maatregelen

Aan de hand van de risico's zijn een aantal maatregelen genomen om ervoor te zorgen dat deze acceptabel zijn. De onderstaande tabel geeft de risico's met de maatregelen weer.

|  |  |  |
| --- | --- | --- |
|  | **Hoofd & Sub Risico** | **Maatregelen** |
| **1** | ***operationele doorgang*** |  |
| **1a** | Ingezet als operationeel medewerker. | Afspraak met de opdrachtgever dat dit niet gebeurd. |
| **1b** | Medewerkers in de operatie hebben geen tijd. | Projectorganisatie bestaat uit drie personen en er is er altijd wel iemand beschikbaar. |
| **1c** | Geen beschikking over OTA straat. | D.m.v. test account in de operationele omgeving kan er toch getest worden. |
| **2** | ***acceptatie werkvloer*** |  |
| **2a** | Management geeft geen akkoord. | Scriptie kan wel geschreven worden op basis van de theorie. |
| **2b** | Management geeft geen draagkracht. | Opdracht is een duidelijke wens en komt van het management af dus zal niet gebeuren. |
| **2c** | Geen acceptatie vanaf de werkvloer. | Meeting met de teamleaders voor verduidelijking. |
| **3** | ***scope (te groot)*** |  |
| **3a** | Opdracht forumlering is te uitgebreid. | Beter afbakenen en verkleining toepassen. |
| **3b** | Oplossing is te globaal. | Verder uitdiepen en specificeren. |
| **4** | ***tijd (project en andere activiteiten)*** |  |
| **4a** | Niet voldoende tijd. | Zie risico 3a. |
| **5** | ***inzetbaarheid projectleider*** |  |
| **5a** | Absentie door ziekte of andere omstandigheden. | Zelf verantwoordelijk voor het beperken hiervan. |

Als laatste zijn de maatregelen opgenomen met de identificatie van de kans, impact en dat is weergegeven in het onderstaande schema.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Hoofd Risico** | | **Sub Risico** | **Kans** | **Impact** |
| **1** | ***operationele doorgang*** |  |  |  |
| **1a** |  | Ingezet als operationeel medewerker. | ***laag*** | ***hoog*** |
| **1b** |  | Medewerkers in de operatie hebben geen tijd. | ***laag*** | ***middel*** |
| **1c** |  | Geen beschikking over OTA straat. | ***laag*** | ***laag*** |
| **2** | ***acceptatie werkvloer*** |  |  |  |
| **2a** |  | Management geeft geen akkoord. | ***laag*** | ***middel*** |
| **2b** |  | Management geeft geen draagkracht. | ***laag*** | ***middel*** |
| **2c** |  | Geen acceptatie vanaf de werkvloer. | ***laag*** | ***middel*** |
| **3** | ***scope (te groot)*** |  |  |  |
| **3a** |  | Opdracht forumlering is te uitgebreid. | ***laag*** | ***middel*** |
| **3b** |  | Oplossing is te globaal. | ***laag*** | ***middel*** |
| **4** | ***tijd (project en andere activiteiten)*** |  |  |  |
| **4a** |  | Niet voldoende tijd. | ***laag*** | ***middel*** |
| **5** | ***inzetbaarheid projectleider*** |  |  |  |
| **5a** |  | Absentie door ziekte of andere omstandigheden. | ***laag*** | ***middel*** |

### Conclusie Risicoanalyse

Door de genomen maatregelen zijn de risico's voor dit project geminimaliseerd en worden als acceptabel beschouwt. Echter dient men wel met de planning bij iedere activiteit rekening te houden dat er mogelijk vertraging op kan treden. Dit omdat de tijdsduur van dit project over een periode van zes maanden bedraagt.

## Kosten-batenanalyse

### Kosten

Voor dit project geldt dat het een zo kosten efficiënt mogelijk project dient te zijn wat de operationele dienstverlening niet verstoord. Dit houdt in dat er nauwelijks of geen kosten gemaakt worden behalve de uren die erin gestoken worden door de projectleden en opdrachtgever.

Een overzicht van de verwachte uren die er door de projectleden in wordt gestoken is hieronder weergegeven.

|  |  |  |
| --- | --- | --- |
| **Opdrachtgever:** | **Functie:** | **Inschatting Uren:** |
| Leon van Toorenburg | Team leader Managed Services Infrastructure Teams | 5 uur |
| **Stuurgroep:** | | |
| Jan Weerts | Lead Consultant Networking & Storage | 150 uur |
| Ben Beens | Security Officer | 50 uur |
| Joep Smets | Compliance Officer | 20 uur |
| **Project leider:** | | |
| Patrick Vaes | Project leider | 700 uur |
| **Overige:** | | |
| Afdeling SE-S | Leden van de afdeling | 5 uur |
| Afdeling SE-NS | Leden van de afdeling | 5 uur |
| Overige Afdelingen | Leden van de afdeling | 5 uur |
| **Totaal Uren door Ciber Managed Services Personeel:** | | 240 uur |

De uren van de project leider zijn in deze niet meegenomen als kosten omdat de project leider niet in dienst is bij Ciber Managed Services en hiervoor niet wordt betaald.

### Baten

Met de uitvoering van dit project zet Ciber Managed Services en grote stap richting de toekomst met betrekking tot veiligheid en het minimaliseren van risico's.

Helderheid met betrekking tot de functionele werkzaamheden van werknemers die dan voor het grootste deel in kaart zijn gebracht. Tevens is er dan ook de mogelijkheid om de medewerkers beter te kunnen monitoren en begeleiden.

# Kwaliteitsborging

## Productkwaliteit

De productkwaliteit per product is hieronder weergegeven en staat in relatie met het project.

* Adviesrapport methoden en technieken:

Een gedegen rapport met methoden en technieken die gericht zijn op Ciber Managed Services waaruit de methode en/of techniek gekozen zal worden voor implementatie.

* Template aan de hand van de gekozen methoden of technieken:

Een beschrijving van de invulling aan de gekozen methode of techniek. Deze om het vervolgens te borgen in het beleid en de visie van Ciber Managed Services.

* Test en implementatie plan:

Hoe het word getest en hoe het wordt ingevoerd met de daarbij behorende resultaten.

* Adviesrapport over de mogelijke invoering overige afdelingen:

Een gedegen rapport met de mogelijk- en onmogelijkheden binnen de andere afdelingen van Ciber Managed Services

## Proceskwaliteit

Door het project bij een persoon neer te leggen wordt het proces continue bewaakt en gewaarborgd. De controle hierop zal worden uitgevoerd door middel van de op te leveren resultaten. Tevens het tweewekelijks contact met de Security Officer evenals het dagelijks contact met de Lead Consultant Networking & Storage speelt hierbij een belangrijke rol.

# Bijlagen

geen.

# Bijlage B Communicatieplan

|  |  |  |  |
| --- | --- | --- | --- |
| **Communicatieplan** | | | |
| **Actiepunt:** | **Datum:** | **Hoe:** | **Opmerkingen:** |
| Voortgangsrapportage met de Security Officer. | 17-02-2012 | Bespreking. | - |
| Voortgangsrapportage met Docent. | 24-02-2012 | Via mail. | - |
| Inleveren PvA en communicatieplan i.o.m. begeleidend docent. | 24-02-2012 | Via mail. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 02-03-2012 | Bespreking. | - |
| Eerste bedrijfsbezoek. | 07-03-2012 | Bespreking in Rosmalen. | K0.11 |
| Bespreken plan van aanpak en communicatieplan. | 07-03-2012 | Bespreking in Rosmalen. | K0.11 |
| Voortgangsrapportage met Docent. | 09-03-2012 | Via mail. | - |
| Adviesrapport methode en technieken. | 09-03-2012 | Via mail. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 16-03-2012 | Bespreking. | - |
| Voortgangsrapportage met Docent. | 23-03-2012 | Via mail. | - |
| Voortgangsrapportage met de Security Officer. | 30-03-2012 | Bespreking. | - |
| Template aan de hand van de gekozen methode of techniek. | 30-03-2012 | Via mail. | Gereed. |
| Voortgangsrapportage met Docent. | 06-04-2012 | Via mail. | - |
| Voortgangsrapportage met de Security Officer. | 13-04-2012 | Bespreking. | - |
| Voortgangsrapportage met Docent. | 20-04-2012 | Via mail. | - |
| Test en implementatie plan. | 20-04-2012 | Via mail. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 27-04-2012 | Bespreking. | - |
| Voortgangsrapportage met Docent. | 04-05-2012 | Via mail. | - |
| Adviesrapport over de invoering op de overige afdelingen. | 04-05-2012 | Via mail. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 11-05-2012 | Bespreking. | - |
| Voortgangsrapportage met Docent. | 18-05-2012 | Via mail. | - |
| Inleveren afstudeerverslag concept. | 18-05-2012 | Via mail. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 25-05-2012 | Bespreking. | - |
| Bespreken afstudeerverslag concept. | 25-05-2012 | Via mail of afspraak. | Gereed. |
| Tweede bedrijfsbezoek/tevens beoordelingsgesprek. | i.o.m. docent en  Jan Weerts. | Volgt. | - |
| Voortgangsrapportage met Docent. | 01-06-2012 | Via mail. | - |
| Inleveren definitief afstudeerverslag in viervoud. | 07-06-2012 | Stage-afstudeerbureau kamer 4.29. | Gereed. |
| Voortgangsrapportage met de Security Officer. | 08-06-2012 | Bespreking. | - |
| Voortgangsrapportage met Docent. | 15-06-2012 | Via mail. | - |
| Bespreken Afstudeervoordracht (PowerPoint presentatie). | 15-06-2012 | Via mail of afspraak. | - |
| Voortgangsrapportage met de Security Officer. | 22-06-2012 | Bespreking. | - |
| Afstudeervoordrachten jun/jul 2012. | 21-06-2012  tot en met 03-07-20 | Zitting 03-07-2012 | Nog te starten. |