Rolgebaseerd autoriseren: effectief sturen op ICT-gebruik

Mr. P.R. Heiden, drs. M. Stultjens en ing. J.A.M. Hermans RE

Het belang van een effectieve sturing op en beheersing van het gebruik van ICT is voor u evident. Zo ook de vaststelling dat deze vrijwel altijd onder de maat is. De organisatie is niet goed in staat te formuleren wie op welke wijze gebruik mag maken van ICT-toepassingen. Het gevolg is een onbetrouwbaar en zeer inefficiënt autorisatiebeheerproces dat niet in staat is de herleidbaarheid van uitgegeven permissies te waarborgen. Met als gevolg dat de ICT-verantwoordelijke het ICT-gebruik niet 'in control' heeft, waardoor er onvoldoende basis is voor sturing en verantwoording. Dit artikel beschrijft niet alleen waarom deze sturing ontoereikend is (en dus goed onderbouwde verantwoording moeilijk mogelijk maakt) ondanks allerlei goedbedoelde doch niet coherente maatregelen en de inzet van vaak peperdure softwarepakketten, maar geeft ook aan hoe met behulp van rolgebaseerd autorisatiemanagement en de juiste tooling effectieve sturing wel mogelijk is.

Inleiding

Boekhoudschandalen zoals bij Enron hebben geleid tot nieuwe regelgeving zoals de Sarbanes-Oxley-wetgeving en de Code Tabaksblat, die weer leiden tot meer intern en extern gerichte controlemaatregelen. De auditwereld heeft de snelle jaren negentig niet kunnen bijhouden en wordt dus nu met grof, zelfs strafrechtelijk geschut tot een inhaalslag gedwongen. Het belang van een betrouwbare inzet van bedrijfsmiddelen zoals onder andere ICT en controle daarop, neemt dus toe. Zo bezien is het opvallend dat het vermogen om het ICT-gebruik te sturen en daarover verantwoording af te leggen, niet toeneemt en in onze ogen zelfs afneemt. Misschien nog opvallender is dat vele ICT-auditors ondertussen geen handreiking bieden om dit groeiende probleem op te lossen. Dit artikel reikt de hand.

Na een uiteenzetting van de oorzaken waardoor controle op autorisaties lastig is, wordt ingegaan op de voortdurende divergentie tussen de intentie van de organisatie (de SOLL) en de praktijk (de IST). Tevens worden de twee hoofdprocessen beschreven, het tactisch en het operationeel autorisatiemanagement, die steeds een actuele vastlegging van SOLL dienen te waarborgen. Vervolgens wordt de rolgebaseerde autorisatiemethode beschreven, inclusief de noodzaak tot geautomatiseerde ondersteuning daarvan. Ten slotte wordt een zich in de praktijk bewezen hebbende aanpak voor de invoering van deze autorisatiemethode beschreven.

Mr. P.R. Heiden
is oprichter en directeur van BHOLD Company, leverancier van rolgebaseerde autorisatiemanagementsoftware. Hij is in 1998 begonnen met de ontwikkeling van software voor overkoepelend rolgebaseerd autoriseren. Daarvoor is hij afgestudeerd in Romeins en Nederlands recht en als bedrijfsjurist werkzaam geweest bij KPN, waarbij hij zich onder meer in een vroeg stadium bezighield met effecten van internet op het handelsverkeer.

p.heiden@bholdcompany.com

Ing. J.A.M. Hermans RE
is werkzaam als senior manager bij KPMG Information Risk Management in Amstelveen. Hij is de KPMG National Service Manager voor Identity Management en heeft de laatste acht jaar vele projecten op het gebied van PKI, e-business en Identity Management uitgevoerd bij diverse grote organisaties in en buiten Nederland. Daarnaast leidt hij de internationale productontwikkeling van KPMG ten aanzien van Identity Management, hetgeen heeft geleid tot de overkoepelende KPMG Identity Management in Control-aanpak.

hermans.john@kpmg.nl

Drs. M. Stultjens
is eveneens directeur van BHOLD Company. Hij is econometrist en afgestudeerd op het onderwerp client-serverdatabaseprogrammatuur, daarna is hij werkzaam geweest als logistiek specialist voor Fokker en is hij bij Exact onder meer verantwoordelijk geweest voor de opbouw van de consultancytak. Vanaf 2001 is hij aan BHOLD verbonden als directeur met speciale aandacht voor marketing en sales.

m.stultjens@bholdcompany.com

Controle is moeilijk

Controle op het gebruik van ICT is niet eenvoudig. De ICT van grote organisaties is veelsoortig en veelal versnipperd. In elke applicatie afzonderlijk wordt bepaald 'wie wat mag'. Degene die voor alle ICT-toepassingen moet bepalen wie wat mag en er ook voor moet zorgen dat elke applicatie dienovereenkomstig is ingesteld, heeft een niet erg benijdenswaardige job. Er zijn gewoonweg te veel bewegende delen om deze taak naar behoren uit te voeren: mensen, ICT-middelen, beleid, regelgeving, alles beweegt, niets kan even worden bevroren om de autorisaties voor het ICT-gebruik in overeenstemming te brengen met de organisatie-eisen en -wensen.

We kunnen misschien niet stellen dat de overeenkomst tussen gewenste toekenning en feitelijke implementatie van autorisaties volledig op toeval berust maar beperkt is de overeenkomst zeker – ook al zorgen vrijwel alle gebruikers ervoor dat ze minimaal de benodigde rechten op de informatiesystemen hebben gekregen. Dit is geen overstatement, ook niet als de ICT-manager het tegenspreekt met het argument dat hij net een (meta-) directory heeft geïmplementeerd. Want een directory lost het werkelijke autorisatieprobleem namelijk niet op, een directory levert efficiëntievoordelen op – zij 'spaart slechts schoenzolen'. Een directory synchroniseert een toevoeging, wijziging of verwijdering van gebruikers (niet hun autorisaties) voor een aantal applicaties, maar de directory (her)kent niet de oorzaak van de wijziging: of dat nu de start van een project is, plotselinge ziekte of ontslag op staande voet. Daarmee wordt dus niet het gewenste verband gelegd tussen het beheer van autorisaties en de daarvoor relevante gebeurtenissen die zich binnen de organisatie afspelen. En dat is de essentie van het probleem: het autorisatiemanagementproces is niet betrouwbaar omdat het geen aansluiting garandeert tussen de intentie van de organisatie en de feitelijke verwerking in de ICT.

Een ICT-manager die zegt dat hij de zaak op orde heeft, heeft een bijzonder stel hersens; een brein dat in staat is tot transcendent communiceren met de gehele organisatie. Die manager zou – met onderbouwing – moeten kunnen aantonen dat hij op elk moment op gedetailleerd en geaggregeerd niveau inzicht heeft in:

- de actuele status van elke gebruiker, ontslagen, aangenomen, van functie gewisseld, op vakantie, op non-actief geplaatst, tijdelijk bezig met een project, waarnemend;
- wat iedere gebruiker in elk systeem wel en niet mag;
- de laatste stand van zaken op het gebied van beleid, wet- en regelgeving, reorganisaties, fusies en overnames, en dergelijke,

en daaraan direct de gewenste gevolgen kan verbinden in de toedeling, wijziging en intrekking van autorisaties.

KPMG Information Risk Management heeft in het najaar van 2003 in samenwerking met het Genootschap van Informatie Beveiligers (GvIB) het eerste grootschalige onderzoek naar Identity Management in Nederland uitgevoerd. Op basis van de reacties kunnen de volgende hoofdconclusies worden getrokken:

- Veel organisaties zijn niet volledig 'in control' wat betreft Identity Management.
- In tegenstelling tot wat met name in de media wordt gemeld, is de voornaamste reden voor het aanpakken van Identity Management niet het bereiken van kostenbesparing, maar het verhogen van gebruikersgemak en het voldoen aan wet- en regelgeving.
- Hoewel binnen veel organisaties (impliciete) Identity Management-processen aanwezig zijn, zijn deze vaak niet geïmplementeerd op een efficiënte en effectieve wijze.
- Veel organisaties hebben geen volledig beeld van toegekende autorisaties. Tevens bestaat de indruk bij de meeste organisaties dat autorisaties te ruim zijn ingesteld, dat wil zeggen gebruikers beschikken over meer autorisaties dan benodigd voor hun functioneren.
- Het merendeel van de organisaties heeft geen inzicht in de (huidige) kosten en baten van Identity Management.

Zie verder het artikel van Koorn en Hermans in deze Compact.

Het niet 'in control' zijn ten aanzien van Identity Management kan leiden tot ernstige beveiligingsincidenten, zoals privacy-incidenten, het openbaar raken van confidentiële informatie alsmede interne fraude. Een dergelijk beveiligingsincident kan een negatieve impact hebben op het vertrouwen van zowel klanten als businesspartners en kan dus concreet omzetverlies betekenen!

Tevens kan het niet 'in control' zijn ten aanzien van Identity Management leiden tot het niet kunnen voldoen aan wet- en regelgeving, zoals daar zijn Sarbanes-Oxley- en privacywetgeving. Het niet kunnen voldoen aan dergelijke wetgeving kan bij incidenten leiden tot aansprakelijkheid van de organisatie en soms zelfs van bestuurders persoonlijk!

Kortom, voldoende redenen om Identity Management gestructureerd aan te pakken.

SOLL en IST[1]

Kort gezegd, de uitdaging is ervoor te zorgen dat het door de organisatie gewenste ICT-gebruik in continuïteit overeenkomt met de feitelijk geïmplementeerde autorisatie-instellingen. In audittermen: de SOLL bepaalt de IST. Verandert de SOLL, dan verandert de IST overeenkomstig mee.

Juist de voortdurende instandhouding van deze causaliteit blijkt voor organisaties in de praktijk vaak onhaalbaar. Dat heeft vooral te maken met een gebrekkige vastlegging van de SOLL, ten gevolge van een inadequaat autorisatiebeheerproces. Organisaties leggen hun SOLL-situatie vast in een functierechtenmatrix. Het is bekend en aanvaard, geen enkele functierechtenmatrix loopt gelijk met de feitelijke toestand:

1. Het gebruikersbestand is te dynamisch om handmatig exact bij te houden wie wat mag en vooral wat diezelfde persoon niet meer mag als hij bijvoorbeeld van functie verandert.
2. De functierechtenmatrix weerspiegelt niet de realiteit omdat iemands formele, hiërarchische functie nu eenmaal maar een beperkt deel van de autorisatiebehoefte bepaalt. Autorisaties vloeien voort uit allerlei situaties, zoals vervanging van een zieke collega, deelname aan een project, een overname of het vervullen van specifieke opdrachten (bijvoorbeeld een onderzoek naar fraude).
3. De praktijk redt zichzelf. Afdelingen zorgen voor anonieme accounts zodat externen of tijdelijke krachten direct aan het werk kunnen of geven aan elkaar het wachtwoord door van een zieke collega. Ondanks de aanwezigheid van de matrix doet iedereen toch gewoon zijn werk.

Niettemin geeft een organisatie een Sysiphus zo nu en dan de Hercules-taak om de IST in overeenstemming te brengen met de SOLL – in de wetenschap dat per direct SOLL en IST weer gaan divergeren.

De inzet van tools om SOLL en IST met elkaar in overeenstemming te brengen leidt vaak tot teleurstellende en soms deerniswekkende resultaten. Dat heeft te maken met een aantal intrinsieke tekortkomingen in de ondersteunende software voor overkoepelend gebruikers- en autorisatiebeheer. De manier waarop de SOLL dient te worden gedefinieerd in deze systemen houdt weinig of geen verband met de realiteit. Zoals hierboven aangegeven zijn er diverse oorzaken waardoor autorisaties niet uitsluitend samenhangen met de functie. De onrealistische definitie van de SOLL-situatie leidt *de facto* tot de onmogelijkheid deze hard (d.w.z. geautomatiseerd) af te dwingen. In feite wordt medewerkers in een organisatie dan het werken onmogelijk gemaakt. Het afdwingen van de SOLL in een 'big bang'-scenario leidt tot aanzienlijke weerstanden en niet zelden tot het vrijwel direct weer terugdraaien naar de oude – weliswaar onvolkomen maar in ieder geval werkbare – situatie. En omdat de SOLL niet goed afdwingbaar is, wordt in feite de IST-situatie weer vastgelegd in het autorisatiesysteem en zijn we terug bij af. De onderbouwing van de investering om de IST via een omweg weer naar de IST over te brengen is de auteurs onbekend, maar deze aanpak wordt vaak 'succesvol' toegepast. Denk bijvoorbeeld aan de succesvolle migraties van kantoorautomatiseringsomgevingen naar Directory Services waarbij de IST-situatie onverkort wordt overgenomen.

1) SOLL: gewenste situatie; IST: huidige situatie (meestal t.a.v. internecontrolemaatregelen).

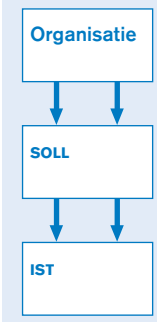
Geen enkele functierechtenmatrix weerspiegelt de feitelijke situatie

Is dat nu allemaal zo'n punt? Voor de Compact-lezers is dat preken voor eigen parochie, maar toch zetten we nog eens kort op een rij waarom dat ook voor de gehele organisatie een punt is (zie verder [Mien03]):

- De geschetste aanpak is inefficiënt. Medewerkers, freelancers, uitzendkrachten en externe projectmedewerkers komen en gaan in een organisatie, maar in de ICT blijven ze. Die vergt meer licenties en meer hardware dan nodig, kortom meer ICT dan strikt noodzakelijk. Dus meer beheer dan nodig, dus meer management dan nodig.
- De geschetste aanpak is risicovol (dus meer regels). Als de SOLL de IST niet stuurt is er in feite geringe sturing, dus geringe controle, dus beperkte grondslag om verantwoording af te leggen over het ICT-gebruik. Vergelijk het met de operationeel directeur van een chemische fabriek die geen inzicht heeft in wie wat kan met zijn naftakraker.

Er is derhalve een serieus bedrijfsbelang om de IST van het ICT-gebruik in overeenstemming te brengen met de SOLL en die situatie ook in stand te houden. De aanpak is op hoofdlijnen relatief eenvoudig (zie figuur 1):

1. Leg steeds de meest actuele SOLL vast.
2. Dwing de SOLL steeds af in de IST.



Figuur 1. Relatie tussen SOLL en IST.

Actuele vastlegging van de SOLL

Wie of wat bepaalt de SOLL eigenlijk? De actuele, gewenste toestand van de autorisaties van elke gebruiker, de SOLL, wordt in feite op twee niveaus bepaald, die elk een eigen proces van vastlegging vragen.

1. Operationeel/gebruikersmanagement

Dit niveau behandelt de toedeling van autorisaties aan personen: Jansen heeft functie K345, dus Jansen krijgt autorisatieprofiel X in het plansysteem en profiel Y in het financiële systeem. Van belang voor de SOLL-vast-

legging is te weten wat de status van Jansen is. Operationele vastlegging van de SOLL houdt direct verband met de actuele vastlegging van de status van elke gebruiker.

Het woord *status* is hier bewust gehanteerd en wordt gebruikt in zijn waardenvrije betekenis. Het gaat hier om de hoedanigheid van een persoon waaraan rechtsgevolgen worden verbonden. Dat wil zeggen dat uit een exacte statusbepaling ook precies de verantwoordelijkheden, bevoegdheden en taken van de betreffende persoon kunnen worden gedestilleerd.

Die status bepaalt de bevoegdheid en de bevoegdheid bepaalt uiteindelijk de set van autorisaties die de gebruiker ter beschikking dient te staan. De status vloeit niet uitsluitend voort uit zijn arbeidsrechtelijke positie. Natuurlijk begrijpt iedereen dat er een direct verband dient te zijn tussen beschikbare autorisaties en ontslagen zijn of het hebben van een verkoop- of administratieve functie. Toch is onze schatting dat dergelijke functiegebonden gegevens nog niet de helft van de autorisatietoedeling bepalen. Van even groot belang is de vandaag opgedragen taak om dossiers te vernietigen, het waarnemen van een collega of de deelname aan een project gedurende drie dagen per week. Maar bijvoorbeeld kan ook van belang zijn of de benodigde opleidingen zijn gevolgd en of deze nog steeds relevant zijn, of dat een geheimhoudingsovereenkomst is getekend voordat tot specifieke informatie toegang wordt gegeven. Al deze gebruikergebonden elementen tezamen bepalen de status van een persoon. En de status bepaalt wat iemand wel of niet mag. Het lastige van de status is dat die op vele plaatsen wordt bepaald en bij voortduring verandert. De status van een persoon kan niet uitsluitend bepaald worden vanuit het personeelssysteem. Niet alle relevante gegevens worden daarin vastgelegd en ze zijn zeker niet voldoende actueel.

Om een actuele SOLL vast te kunnen leggen is het in de eerste plaats van belang dat elke relevante impuls ('event') voor statusbepaling kan worden opgeslagen. Dat betekent dat die vastlegging open moet zijn. Open voor impulsen uit personeelssystemen, open voor beslissingen van lokaal management, niet alleen uit de lijn maar ook in projecten, om bijvoorbeeld iemand te schorsen of tijdelijk toe te wijzen aan een speciale taakgroep. Maar misschien op termijn ook wel voor externe impulsen zoals een verandering van nationaliteit, intrekking van een rijbewijs of het ontstaan van (gedeeltelijke) arbeidsongeschiktheid. Al die gegevens samen bepalen de status van de gebruiker en daarmee de bevoegdheid tot ICT-gebruik, en aldus uiteindelijk de meest gewenste autorisaties in een gecontroleerde ICT-omgeving.

Het bijhouden van statusgegevens (persoonsgebonden attributen) vormt de sleutel tot dynamisch of contextgebonden autoriseren. Naarmate de mogelijkheden van gebruikers toenemen om handelingen te verrichten met verreikende consequenties, wordt deze vorm van autoriseren steeds belangrijker. Uiteindelijk geldt dit natuurlijk ook voor wat in de ICT-wereld de *'extended enterprise'* wordt genoemd. Voor een organisatie is het ook van belang voortdurend de status te kennen van allerlei typen derden, zoals leveranciers, joint ventures, klanten, aandeelhouders en toezichthouders. Ook zij zijn immers meer en meer actieve gebruikers van de ICT-omgeving van diezelfde organisatie. Ook over hun ICT-gebruik moet verantwoording worden afgelegd. Voor nu is het al moeilijk genoeg om binnen de *'enterprise'* te komen tot een adequate actuele statusvastlegging, maar het is zeker niet visionair om reeds rekening te houden met de groeiende noodzaak deze statusvastlegging ook voor buitenstaanders te waarborgen. Dat betekent in feite dat gekoppeld moet kunnen worden met bronnen van buiten de organisatie waarvandaan relevante impulsen komen.

2. Tactisch management

Het tactische niveau ziet in tegenstelling tot het operationele niveau juist toe op de toekenning van autorisaties, *zonder aanzien des persoons*. We kijken niet meer naar de aanvrager (of harder gesteld, naar zijn sociale vermogens om wat gedaan te krijgen van de systeembeheerder), maar we kijken naar het statustype en koppelen aan die gedepersonaliseerde typering gewenste gevolgen voor het ICT-gebruik.
Als de status van een gebruiker bepalend is voor zijn bevoegdheden (en dat is natuurlijk gewenst) en een onderneming is in staat steeds de meest actuele status van een gebruiker vast te leggen, dan is het mogelijk het gewenste effect in autorisatie-instellingen en dus in het ICT-gebruik te automatiseren. Door dat te doen verschuift voor de ICT-manager het belang van het verschaffen van de juiste autorisaties aan de juiste personen naar een veel minder hectische en overzichtelijker opdracht, namelijk instelling van de juiste regels om steeds aan de status van een gebruiker de gewenste autorisaties te koppelen.

De regels hierboven zijn in feite een weergave van het beleid. Beleid dat voortvloeit uit een taakstelling. Er moet een samenhang zijn tussen de opgedragen taken van, zeg, een sales manager en de aan hem ter beschikking gestelde autorisaties. In feite dient de toekenning van ICT-middelen volledig volgend te zijn aan de autonome besluitvorming in de organisatie. Sterker gezegd, beleid wordt overal bepaald maar per definitie niet in het hoofd van de beheerder van de regels. Beleid inzake het ICT-gebruik wordt bepaald op businessniveau, bij

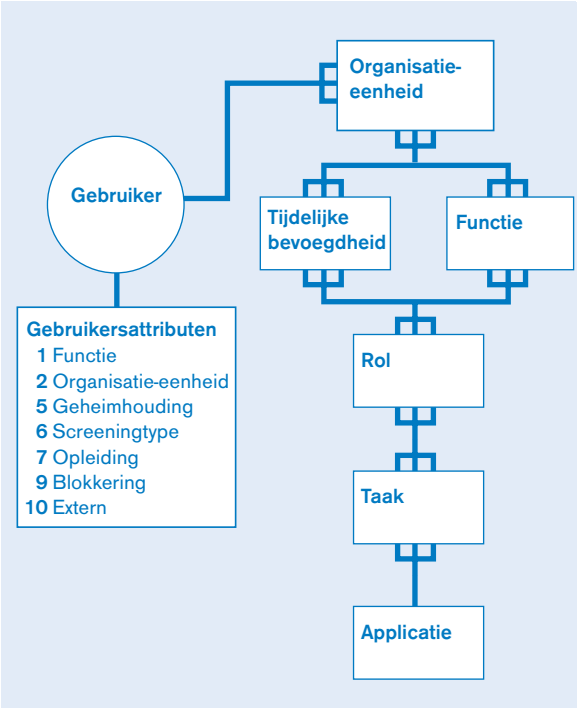
personeelszaken, bij juridische zaken, bij beveiliging. Kortom, de regels die bepalen welke autorisaties aan welke status gekoppeld dienen te worden, moeten een uitdrukking zijn van businessintenties en dus uitdrukbaar in de taal van de mensen die beleid maken en wijzigen. Dat is precies wat rolgebaseerd autorisatiemanagement doet.

Rolgebaseerd autorisatiemanagement, de taal van de business, de basis van de SOLL

Hoe verbindt een organisatie aan de status van een gebruiker bevoegdheden? Een organisatie bepaalt de inhoud van bevoegdheden aan de hand van de bedrijfsprocessen waarin iemand een rol speelt. De administratief medewerker speelt een goed omschreven rol in bijvoorbeeld financiële processen, maar diezelfde persoon kan evenzeer vertrouwenspersoon zijn voor de medewerkers van de buitendienst en heeft dan een volledig afwijkende rol.
Vrijwel iedereen heeft meerdere rollen in een organisatie. Nu is het mooie van rollen dat die heel wat stabieler zijn dan personen. Aan een rol kunnen we bevoegdheden hangen zonder dat die rol aan voortdurende verandering onderhevig is. De rol is bij uitstek het middel waaraan men regels kan hangen ten aanzien van toe te delen autorisaties: heeft iemand rol A dan weet ik dat hij in het financiële systeem profiel X heeft en in het ordersysteem profiel Y. Dit vormt de kern van RBAC, Role-Based Access Control, een methode om de kloof tussen businessintenties en ICT-begrip te overbruggen, met andere woorden de kloof tussen SOLL en IST.

In meer abstracte termen werkt RBAC als volgt: een applicatie kent autorisaties of *taken*, een set taken uit een applicatie vormt een systeemrol, een set systeemrollen (vaak uit verschillende applicaties) vormt een organisatierol. Systeemrollen en organisatierollen verschillen structureel. Systeemrollen sluiten aan bij ICT-terminologie, organisatierollen sluiten aan bij taakstelling in een bedrijfsproces. De organisatierol koppelen we aan de persoon die daar op basis van zijn status toe bevoegd is. In deze rolmodellering wordt een haarscherp onderscheid gemaakt tussen systeem- en organisatierollen. Systeemrollen maken het leven van de ICT'ers gemakkelijk, organisatierollen het leven van de verantwoordelijke manager. Juist op dit punt wordt de kloof overbrugd tussen ICT en de rest van de organisatie.

Omdat organisaties die behoefte hebben aan een dergelijke ordening vaak meer dan duizend medewerkers in dienst hebben, ligt het voor de hand binnen de combinatie gebruiker – rol(len) een extra ordening aan te brengen, precies zoals de organisatie dat ook doet: de organisatie-eenheid (lees afdeling, projectgroep, OR, locatie, etc.). In feite worden rollen beschikbaar gemaakt in organisatie-eenheden, namelijk die welke de organisatie-eenheid nodig heeft om de opgedragen taken goed uit te voeren. In feite komt het er dus op neer dat gebruikers in organisatie-eenheden worden ondergebracht en daarbinnen de rollen krijgen die hen op basis van hun status toekomt. De verbinding van een rol aan een persoon stelt ons vervolgens in staat de autorisaties te activeren waaruit de geactiveerde rollen zijn opgebouwd. In figuur 2 is dit weergegeven, waarbij met het type verbinding tussen de entiteiten (enkelvoudige of drievoudige lijn) is aangegeven of het een 1-op-1 of 1-op-N relatie betreft.



Figuur 2. Organisatorisch relatiediagram.

Kortom, een organisatie heeft om redenen van beheersing, beveiliging en efficiëntie concreet baat bij:
a. een voortdurend actuele vastlegging van de SOLL;
b. een voortdurend met de SOLL in overeenstemming gebrachte IST.

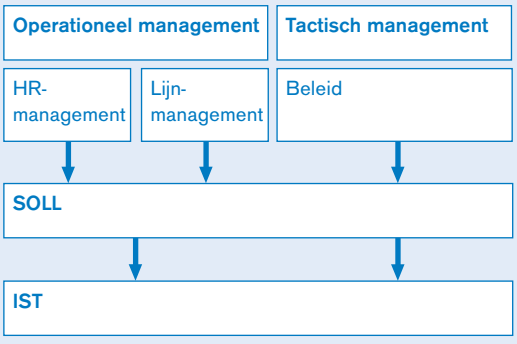
Geautomatiseerd operationeel management

We hebben net vastgesteld dat de RBAC-methode bij uitstek geschikt is om de organisatie in staat te stellen duidelijk te instrueren wie op welk moment met welke status precies wat mag, de SOLL. Zoals we al eerder zagen is de grote uitdaging vervolgens de SOLL steeds actueel te houden. Daarvoor is geautomatiseerde ondersteuning ons inziens vrijwel onontbeerlijk. De complexiteit en omvang van het rolgebaseerde model in combinatie met een hoge frequentie van gebruikers- en statuswijzigingen maken dat een handmatige vastlegging niet realistisch is. De daarvoor in te zetten applicatie moet ervoor instaan dat de vastlegging van operationele en tactische beslissingen steeds de meest actuele gewenste situatie

weerspiegelt en dat deze situatie zonder vertraging in de IST doorwerkt (wordt 'gepropageerd').

In het laatste zinsdeel schuilt een essentieel element: het propageren of de directe doorwerking van wijzigingen van de SOLL in de IST is bepalend voor het vermogen van een organisatie om een betrouwbare verantwoording af te kunnen leggen over het ICT-gebruik. Elke schakel die zich bevindt tussen een bepaling van de SOLL en de uiteindelijke doorwerking daarvan in de IST, vormt een risico. Denk aan de stapel formulieren voor wijzigingen die bij de beheerder blijft liggen voor verdere registratie. Hoeveel daarvan worden onjuist, niet of te laat verwerkt? Hoeveel daarvan worden verwerkt zonder inperking of verwijdering van bestaande autorisaties? Juist deze inherent onbetrouwbare verwerking maakt het afleggen van verantwoording voor het (senior) management riskant.

Voor een applicatie die zorgt voor de vastlegging van de SOLL is het op operationeel niveau nodig dat alle voor de status van een persoon relevante impulsen worden vastgelegd. Dat betekent dat een personeelssysteem direct gekoppeld dient te worden aan deze vastlegging. Dat is relatief eenvoudig. Maar het betekent ook dat impulsen verwerkt worden vanuit andere bronnen, zoals opleidingsdatabases en klant- en relatiesystemen, teneinde steeds de meest actuele status vast te leggen.
Diezelfde applicatie moet ook in staat zijn aan relevante managementbeslissingen direct de gewenste impact in de IST te geven. Dat is minder eenvoudig. Om managementbeslissingen te activeren worden formulieren gebruikt of telefoontjes naar systeembeheerders ('doe maar wat De Vries van Financiën ook mag') of via anonieme accounts (bij ons staat altijd account user 1 tot en met 6 klaar voor externen en het wachtwoord is 'koffiepot').
Het is zaak managementbeslissingen over rollen, verantwoordelijkheden en bevoegdheden ook daadwerkelijk vast te laten leggen door de beslisser zelf. Hij activeert rollen (en daarmee autorisaties) voor zijn medewerkers en weet dat de systeemautorisaties direct dienovereenkomstig zullen worden ingesteld. De vastlegging van operationele managementbeslissingen in de SOLL moet gedelegeerd worden naar lijn- of projectmanagers. Dit brengt met zich mee dat de presentatie van de te activeren autorisaties volledig moet aansluiten bij de belevingswereld van juist dit type gebruiker: geen gebruik van ICT-terminologie, maar met duidelijke referenties naar organisatiebegrippen. Ziehier de noodzaak van een applicatie die op basis van rollen zorgt voor de meest actuele vastlegging van de SOLL en deze vervolgens omzet in instructies aan de onderliggende ICT-systemen.



Figuur 3. Verhouding tactisch en operationeel management.

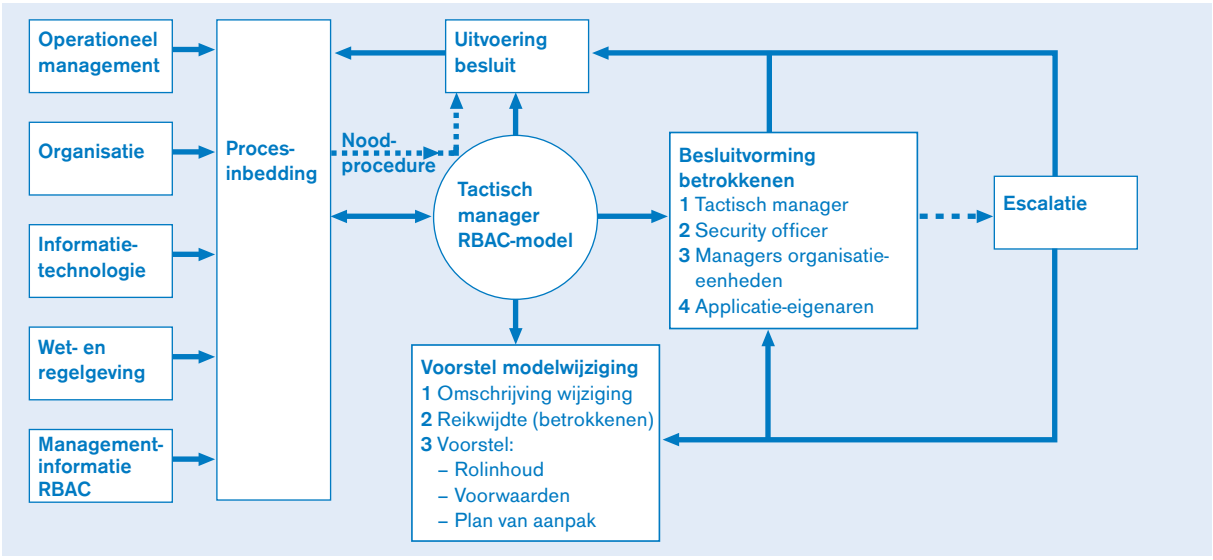
De nieuwe uitdaging, tactisch management

De beschikbaarheid van de juiste set met rollen voor de organisatie-eenheid waarover de verantwoordelijk manager de scepter zwaait, is het resultaat van tactische beslissingen. Tactische beslissingen vormen de andere zijde van de SOLL-vastlegging. Tactische beslissingen betreffen de inrichting en het beheer van RBAC. Het belangrijkste gevolg van de invoering van RBAC is dat de nadruk voor de ICT-organisatie verschuift van hoogfrequente operationele handelingen naar het soms complexe tactisch management, met een vaak onverwacht grote reikwijdte.

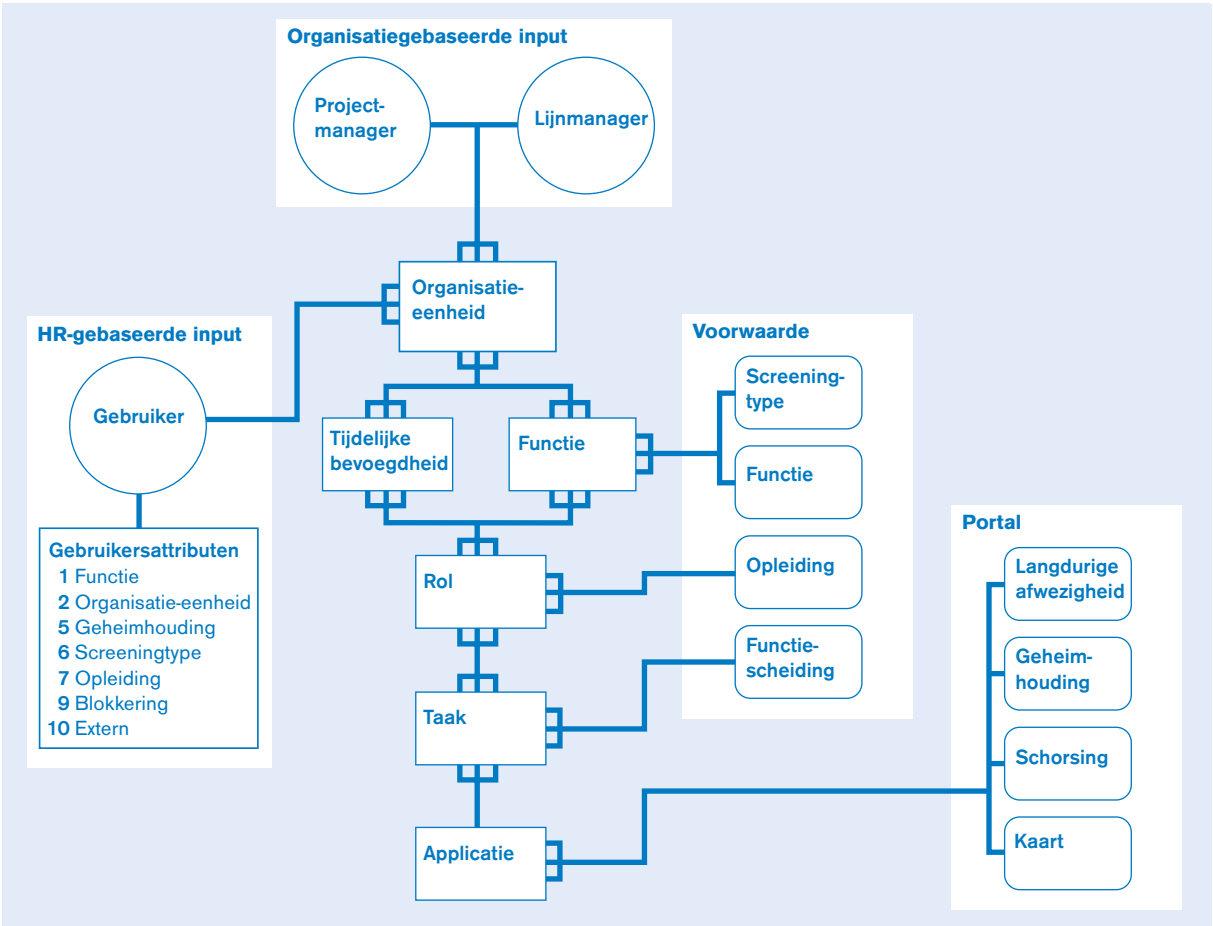
We zagen al dat het doorvoeren van tactische beslissingen bij een rolgebaseerd model neerkomt op het aanpassen van het model zonder aanzien des persoons. We kijken daarbij steeds naar twee bewegende delen:
- Allereerst kijken we naar de inhoud van de rol, dat wil zeggen naar de set van autorisaties (taken of systeemrollen) die gekoppeld is aan de rol. Die inhoud wordt bepaald op basis van wat nodig is voor een goede uitoefening van die rol in een businessproces.
- Daarnaast kijken we naar de voorwaarden waaronder de rol daadwerkelijk aan een persoon kan worden gekoppeld, dat wil zeggen welke attributen een persoon moet hebben (een bepaalde opleiding, functie, groepslidmaatschap en wat ook verder dat de status van een persoon bepaalt) of dat bijvoorbeeld expliciete toestemming van een lijnmanager noodzakelijk is of dat vereisten van functiescheiding of 'chinese walls' in acht worden genomen.

Deze tweedeling tussen de invloed van tactische en operationele managementbeslissingen op gewenste of feitelijke autorisaties is in figuur 3 weergegeven.

De doorvoering van wijzigingen in de SOLL vanwege tactische beslissingen vloeit dus voort uit beleidsbepaling. Dit betekent dat:
- de uitvoerder van tactische beslissingen (tactisch manager) een passieve taakopvatting dient te hebben, hij maakt tenslotte het beleid niet;
- de tactisch manager dient te waarborgen dat hij de meest actuele stand van zaken kent inzake het beleid. Die waarborging vraagt om procedures. In figuur 4 is



Figuur 4. Tactisch RBAC-model.



Figuur 5. RBAC-basismodel.

een beheerschema opgenomen als voorbeeld van dergelijke procedures.

De strikte scheiding van operationeel en tactisch management heeft nog een ander, veelal onderbelicht effect. De vaak vertragende workflows rondom autorisatietoekenning worden grotendeels overbodig! Immers, de workflow strekt er vaak toe om een operationele beslissing (manager wil De Vries autorisatieprofiel X geven) tactisch te toetsen (dat kan wel mits wordt voldaan aan de eisen 1, 2 en 3). In feite wordt de tactische toetsing volledig geautomatiseerd toegepast in de RBAC-applicatie. De toekenning van autorisatie aan De Vries door zijn manager wordt al volledig getoetst door een verificatie van zijn status (die bijvoorbeeld vermeldt dat het vereiste certificaat is behaald of een geheimhoudingsverklaring is getekend). RBAC maakt een einde aan individuele, toevallige, en hierdoor onbeheersbare toekenning van gebruikersrechten.

Modelwijzigingen worden doorgevoerd door de tactisch manager in overleg met de betrokken managers van organisatie-eenheden en applicatie-eigenaren (volgens bovenstaande procedure). Dergelijke wijzigingen gaan juist hen aan, het betreft hun medewerkers respectievelijk hun applicaties. De eigenlijke modelwijziging is vaak een kleine handeling, maar heeft vaak grote gevolgen.

Om kort te gaan, de vastlegging van een immer actuele SOLL dient op twee niveaus te gebeuren:
1. *Operationeel*. De juiste persoon heeft de juiste autorisaties, hetzij afgeleid uit medewerkerregistraties ('user repositories'), hetzij afgeleid van directe managementbeslissingen.
2. *Tactisch*. Het actuele beleid bepaalt aan welke rol welke autorisaties worden verbonden en onder welke voorwaarden die rol ook daadwerkelijk beschikbaar komt voor koppeling aan een persoon.

In figuur 5 is de SOLL-vastlegging gevisualiseerd.

Een dergelijk model wordt ondergebracht in een separate applicatie die zorgt voor met name:
- RBAC-gewijze vastlegging van de SOLL;
- toepassing van de juiste regels om tot autorisatiebeslissingen te komen;
- precieze instructies aan bijvoorbeeld directories of de autorisatiemanagementmodules in backoffice- of andere legacy-omgevingen.

RBAC in de praktijk: de politie

De aard van de aan de politie opgedragen taken maakt de sturing op het gebruik van informatie bijzonder complex. Aan de ene kant is er de voortdurende noodzaak tot directe actie, die vraagt om snelle ruime beschikbaarheid van alle middelen, natuurlijk inclusief informatie; aan de andere kant de noodzaak om geheimhouding te betrachten en exact te handelen in overeenstemming met wet- en regelgeving om zaken überhaupt tot een goed einde te kunnen brengen.

Informatievoorziening bij de politie is dus zeilen tussen Scylla en Charibda. Sturing op de terbeschikkingstelling van informatie moet scherp en snel. In essentie komt dit neer op een snel, precies en betrouwbaar autorisatiemanagementproces dat in staat is te zorgen voor een onmiddellijke en adequate voorziening van informatie aan de individuele medewerker (operationeel proces) met inachtneming van alle toepasselijke (beleids)regels (tactisch management).
Een proces dat een dergelijke tweeledige sturing moet bieden, verdraagt niet allerlei tussenschakels en behoeft automatische ondersteuning om een volstrekt betrouwbare uitkomst te waarborgen. Tussen de intentie van de organisatie ten aanzien van het gebruik van IT en de feitelijke instelling van autorisaties mag geen enkel hiaat zitten. De eis van directe sturing maakt dat zo'n proces niet anders kan worden ingericht dan op basis van rollen, om betrouwbaarheid en directe sturing mogelijk te maken, en geautomatiseerd moet verlopen, om de gewenste snelheid in afwikkeling te realiseren.

In 2003 is de politie gestart met de invoering van RBAC als basis voor haar autorisatiemanagementproces. Per regio wordt een gecontroleerde overgang voorzien van een procedureel beheer op basis van een functierechtenmatrix naar een geautomatiseerd proces waarbij autorisaties op basis van rollen worden toebedeeld. Leerzaam is dat tijdens de selectie van ondersteunende tooling meer en meer duidelijk werd dat het vermogen om de organisatorische realiteit te vangen in een model, doorslaggevend is voor een succesvol verloop van een in essentie changeproject voor autorisatiemanagementprocessen. De praktijk van alledag vraagt nu eenmaal:
- dat gebruikers lid zijn van meerdere organisatie-eenheden (niet alleen de lijneenheid maar ook bijvoorbeeld projecteenheden) en eenvoudig in staat worden gesteld om taken van collega's waar te nemen of aan anderen over te dragen;
- dat autorisaties afhankelijk kunnen worden gemaakt van bijvoorbeeld een gevolgde opleiding, functiescheiding of bepaalde screening, maar dat diezelfde eisen weer door managers doorkruist kunnen worden als de praktijk daarom vraagt.

Invoering van de SOLL: het overbruggen van de kloof, closing the gap

Een goede RBAC-applicatie stelt een organisatie in staat bij voortduring de meest actuele SOLL vast te leggen voor haar ICT-gebruik. Dan nog steeds is daarmee niet het probleem opgelost van de kloof die gaapt tussen SOLL en IST. Een directe afdwinging van de SOLL in de IST is onverantwoord. Immers, we weten dat de organisatie haar werk doet maar we weten niet in hoeverre de daarvoor ter beschikking gestelde middelen ook daadwerkelijk overeenkomen met de gewenste toestand. Uit onze praktijkervaringen met ICT-audits alsmede met verbeterprojecten van het autorisatiemanagement blijkt dat er eigenlijk altijd een groot gat bestaat tussen gewenste en feitelijke situatie. Daarmee is het onverantwoordelijk een theoretische SOLL direct af te dwingen in de IST. Het dichten van de kloof moet beheerst gebeuren, anders treden er vrijwel zeker operationele verstoringen op. Het vermogen om deze kloof beheerst te dichten, met aanvaardbare consequenties voor de organisatie, vormt in feite het sleutelelement van een succesvol project. Om dit te realiseren heeft de Nederlandse Identity Management-specialist BHOLD Company een methode ontwikkeld, bestaande uit de volgende drie hoofdfasen:

1. definitie gewenste situatie (de SOLL);
2. convergentie gewenste en feitelijke situatie (de IST);
3. sturing vanuit de SOLL, voortdurende audit op de IST.

We beschrijven de methode hieronder fasegewijs.

1. Definitie gewenste situatie (de SOLL)

Aan de hand van de bedrijfsprocessen en, voorzover aanwezig, de functierechtenmatrix worden de relevante rollen geïdentificeerd. Deze rollen worden gepaard aan de organisatie-eenheden die personeel hebben dat een dergelijke rol bekleedt of kan bekleden. Aan de rollen worden ten slotte de autorisaties (taken) gekoppeld. Deze opzet wordt ondergebracht in een rolgebaseerd autorisatiemodel. Dit model wordt geverifieerd per organisatie-eenheid met de betrokken managers en applicatie-eigenaren en waar nodig aangepast. Vervolgens worden per afdeling gebruikers aan de voor die afdeling beschikbare rollen gekoppeld.

Het autorisatiemodel hoeft bepaald niet perfect te zijn. Ook in een zeer rudimentaire staat is dit model goed bruikbaar. Uiteindelijk strekt de hele methodiek ertoe om beheerst de overgang naar de SOLL te maken. Dit brengt met zich mee dat in die overgang ook de SOLL veelvuldig wordt aangepast, geperfectioneerd en dichter bij de praktijk gebracht. Dat is voor veel organisaties met slechte ervaringen met een 'big bang'-invoering een geruststellende gedachte.

Op basis van dit autorisatiemodel kan vervolgens de administratie van autorisaties worden beheerd. Aanvragen voor nieuwe gebruikers of nieuwe rechten, dan wel de wijziging of intrekking, worden bijgehouden in het model. Dit kan via formulieren, volledig geautomatiseerd vanuit het personeelssysteem of volgens een tussenvorm. Normaal gesproken zijn deze processen reeds aanwezig (vaak op de helpdesk ingevoerd) en is slechts een beperkte aanpassing en formalisering noodzakelijk. Op hetzelfde moment worden de tactische processen voor het beheer van het autorisatiemodel geïmplementeerd. Implementatie en formalisering van de tactische processen zijn noodzakelijk voor wordt overgegaan naar fase 2.

2. Convergentie gewenste en feitelijke situatie (de IST)

Het resultaat van de eerste stap is dat de organisatie een voortdurend actuele vastlegging heeft van de naar beste inzicht, rudimentair vastgelegde SOLL van de autorisaties. Door nu het model te vergelijken met de autorisatiemodules van de informatiesystemen is het mogelijk de gewenste situatie af te dwingen. Ervaring leert dat SOLL en IST zoveel verschillen dat een directe afdwinging uiterst ingrijpend is voor eindgebruikers, derhalve voor de helpdesk en dus bovenal voor het project zelf. En dat is precies de reden waarom zoveel RBAC-projecten nooit verder dan de Proof of Concept- of pilotfase komen. Met veel enthousiasme worden de organisatorisch toegekende gebruikersrechten gepropageerd naar drie verschillende informatiesystemen in een testomgeving, waarna iedereen zich afvraagt hoe het vervolgens verder moet. Als organisaties niet aanvaarden dat er een groot verschil is, een delta, tussen gewenste en feitelijke organisatie, mislukt elke invoering van RBAC. De delta is er nu eenmaal vanwege de onhaalbaarheid van de aan systeembeheerders en security administrators opgedragen taak en is zeker geen door hen veroorzaakt probleem.

Het komt regelmatig voor dat tienduizenden verschillen worden aangetroffen, maar het blijkt ook dat deze soms al binnen twee weken zijn verholpen. Het grootste deel van de inconsistenties blijkt voor een kenner van het betreffende systeem heel begrijpelijk en dus ook snel verholpen. Inconsistenties kunnen op twee manieren worden weggewerkt, hetzij door aanpassing van de IST-situatie (bijvoorbeeld weghalen oude accounts), hetzij door aanpassing van het autorisatiebeleid (bijvoorbeeld alle medewerkers van afdeling X krijgen toegang tot deze NT-share). Deze laatste variant is een tactische beslissing en komt dus via de toepasselijke tactische procedures tot stand. In dit type wijziging is de besluitvaardigheid van de organisatie veruit het grootste projectrisico.

Er zijn mensen die menen dat de SOLL moet worden gedefinieerd op basis van *'role mining'*. Hiermee bedoelen zij dat van elke applicatie de autorisaties in een separate database worden gekopieerd om daarna op basis van patronen een SOLL te definiëren. Wantrouw hen, zelfs als zij grote geschenken in het vooruitzicht stellen. Het grootste geschenk is voor hen: het onvoorstelbaar grote aantal uren dat besteed wordt aan patroonherkenning teneinde een gesublimeerde versie van de IST uit de IST op te leveren als een SOLL. Zo'n werkwijze valt niet te billijken, het verband met beleid, met intenties van de organisatie, wordt niet gemaakt.

3. Sturing vanuit de SOLL, voortdurende audit op de IST

Per applicatie wordt in fase 2 de delta weggewerkt. Wanneer dit is voltooid, kan vanaf dat moment deze applicatie volledig worden gestuurd vanuit de SOLL. Sturing vanuit een voortdurend actuele SOLL op het ICT-gebruik is de ultieme doelstelling van de ICT-auditor. Maar belangrijker is dat de ICT-auditor kan vertrouwen op de verantwoording die de directie aflegt over het gecontroleerde ICT-gebruik en dat de directie zo met recht kan vertrouwen op de juistheid van haar verslaglegging terzake. Voor die zekerheid moet echter nog een stap worden gezet, die alleen maar kan gebeuren omdat er een strikte scheiding tot stand is gebracht tussen de SOLL en de IST. Omdat de SOLL steeds actueel wordt vastgelegd, is het mogelijk voortdurend ook de consistentie met de IST te bewaken. Verandert er iets in de IST, bijvoorbeeld de activering van een administratorrecht, zonder dat daarvoor een rechtvaardiging is te vinden in de SOLL, dan kan geautomatiseerd de gewenste toestand weer worden hersteld. Juist geautomatiseerde continue bewaking van het behoud van deze consistentie vormt de basis voor sturing van en verantwoording over het ICT-gebruik.

Organisaties zijn aanvankelijk vaak wat terughoudend als het aankomt op de geautomatiseerde afdwinging van de SOLL in de IST. Hoewel dit een begrijpelijke reactie is bestaat daar maar weinig grond voor. Aan de vastlegging van operationele beslissingen ligt per definitie duidelijk beleid ten grondslag. Voor de activering van administratorrechten kan bijvoorbeeld zijn afgesproken dat zo'n autorisatie uitsluitend beschikbaar komt na expliciete goedkeuring van de verantwoordelijke ICT-manager. Omdat deze manager in staat is per direct daaraan te voldoen is dat ook geen enkel probleem. Voor de creatie van een administratorrecht buiten deze procedure om bestaat geen rechtvaardiging. Dientengevolge kunnen deze rechten onmiddellijk ongedaan worden gemaakt.

Conclusie

Om het verband te herstellen tussen de aangeboden ICT-gebruiksmogelijkheden en de intenties van de organisatie is het noodzakelijk dat de afstemming tussen organisatie en ICT over gebruikersrechten accuraat en gedetailleerd is. RBAC maakt dat mogelijk en dat is de grootste toegevoegde waarde. Dat hiermee ook de basis wordt gelegd om verantwoording af te leggen over het gebruik van ICT-middelen en daarmee bij te dragen aan de naleving van vigerende wet- en regelgeving als Sarbanes-Oxley, Basel II, Tabaksblat, IFRS, ROB[2], privacy en dergelijke, is dan eigenlijk van ondergeschikt belang.

Om een actuele SOLL op basis van RBAC effectief te beheren is een specifieke applicatie nodig die losstaat van de IST teneinde een permanente monitoring en auditing tot stand te kunnen brengen van de overeenstemming van SOLL en IST. Die applicatie moet organisaties in staat stellen operationele beslissingen hetzij automatisch (via HRM) te nemen, hetzij door de feitelijk verantwoordelijke manager. Juist deze zo essentiële delegatie is een belangrijk voordeel van rolgebaseerd autoriseren. Daarnaast moet die applicatie in staat zijn duidelijk de reikwijdte van voorgenomen beleidsbeslissingen te tonen en bij doorvoering ook een effectieve afdwinging garanderen. Zo wordt de basis gelegd voor een voortdurend actuele vastlegging van de door de organisatie gewenste toestand. Iedereen die meent dat directories organisaties daartoe in staat stellen, ziet over het hoofd dat directories uitsluitend onderdeel van de IST zijn. Een directory beschikt eenvoudigweg niet over functionaliteit voor een gedegen vastlegging en beheer van organisatorisch toegekende autorisaties.

Het onvermogen om de kloof te overbruggen die nu gaapt met die meest gewenste toestand is de belangrijkste drempel voor een succesvolle implementatie van RBAC. De scheiding van SOLL en IST maakt met een RBAC-toepassing de gestructureerde overgang van een ongestuurde naar een vanuit de SOLL gestuurde ICT mogelijk. Die overgang opent de weg naar verantwoord gebruik van het bedrijfsmiddel ICT, naar efficiënte implementatie van het beveiligingsbeleid, naar effectieve afdwinging van de naleving en naar (pas dan) verantwoording over de inzet van ICT. Met de hier beschreven methode kan die weg met vertrouwen worden afgelegd. En zo reikt de ICT-auditor de hand om niet langer met de vinger te hoeven wijzen.

Literatuur

[Mien03] Ing. P. Mienes RE en B. Bokhorst RE RA, *De (on)beheersbaarheid van toegangsbeveiliging*, Compact 2003/1.

2) ROB: Regeling Organisatie & Beheer, geldend voor Nederlandse financiële instellingen.