In control ten aanzien van uw autorisatie-management

Het huis op orde krijgen en houden op een effectieve en efficiënte wijze

Ing. J.A.M. Hermans RE, drs. D.B. van Ham CISA en drs. J. ter Hart

'In control' ten aanzien van autorisatiemanagement is een vereiste vanuit steeds stringenter wordende wet- en regelgeving, zoals Sarbanes-Oxley (SOX), Basel II en privacywetgeving. In dit artikel wordt beschreven op welke wijze organisaties effectief en efficiënt het voldoen aan deze vereisten aan kunnen tonen ('compliance verification') om vervolgens het huis structureel op orde te krijgen en te houden. Autorisatiemanagement op basis van het concept rolgebaseerd autoriseren kan hierbij een belangrijke rol spelen. In dit artikel wordt vooral ingegaan op de praktische kant van het onderwerp, gebaseerd op een aantal concrete praktijkvoorbeelden. Daarnaast wordt de relatie toegelicht met het thema Identity & Access Management (IAM).

Inleiding

Al zolang organisaties gebruikmaken van informatietechnologie speelt de toegangsverlening tot de informatie van de organisatie een belangrijke rol. Informatie is tegenwoordig één van de meest waardevolle 'assets' van een organisatie. Zonder de juiste informatie worden foutieve beslissingen genomen, kan het bedrijfsproces niet goed worden uitgevoerd, worden klanten minder goed geholpen of wordt schade geleden. Uiteraard speelt hierbij ook het voldoen aan wet- en regelgeving, zoals SOX en Basel II, een belangrijke rol. Het is dus zaak dat iemand over de juiste informatie kan beschikken en dat onbevoegden geen toegang hebben tot informatie, bijvoorbeeld financiële gegevens, klantgegevens en informatie die wordt gebruikt voor de besturing en uitvoering van de primaire processen.

Met het steeds complexer wordende applicatielandschap, fusies en overnames en eisen van de business ten aanzien van IT is het voor organisaties een voortdurende uitdaging om de autorisaties op orde te krijgen, en die ook op orde te houden. In dit artikel wordt een aanpak geschetst van de wijze waarop de organisatie de enorme brij aan foutieve autorisaties op orde kan krijgen en de juiste autorisaties daarna ook op orde kan houden. Dit laatste wordt vaak vergeten of hiervoor wordt niet tijdig een proces ingericht. Het gevolg hiervan is dat jaarlijks projecten worden opgestart om de autorisaties te schonen. Dit levert veel frustraties op aan zowel de IT- als de businesskant en slokt bovendien te veel tijd op. Hierdoor komen medewerkers niet aan hun primaire taken toe en wordt compliance onnodig duur.

Ing. J.A.M. Hermans RE
is senior manager bij KPMG IT Advisory te Amstelveen. Binnen KPMG is hij National Service Manager Identity & Access Management en heeft hij in de laatste jaren vele projecten op het gebied van Identity & Access Management en PKI uitgevoerd bij diverse grote organisaties in en buiten Nederland. Daarnaast leidt hij de internationale productontwikkeling van KPMG ten aanzien van Identity & Access Management, hetgeen heeft geleid tot de overkoepelende KPMG 'Identity & Access Management in Control'-aanpak.

hermans.john@kpmg.nl

Drs. D.B. van Ham CISA
is als manager werkzaam bij KPMG IT Advisory te Amstelveen. Hij richt zich in het bijzonder op adviesdiensten rondom het thema Identity & Access Management (IAM) en project- en programmamanagement op het raakvlak van IT-management en informatiebeveiliging.

vanham.dennis@kpmg.nl

Drs. J. ter Hart
is adviseur bij KPMG IT Advisory te Amstelveen. Hij heeft ruime ervaring met advies- en auditopdrachten op het gebied van Identity & Access Management, elektronische handtekeningen, IT Service CMM, elektronisch factureren en privacy. Daarnaast is hij co-auteur van een witboek voor de Nederlandse overheid inzake het toepassen van Privacy Enhancing Technologies.

terhart.joris@kpmg.nl

Autorisatiemanagement – merendeel van de organisaties onvoldoende 'in control'

Een enquête van KPMG uit 2006, waarin ongeveer duizend verantwoordelijken voor IT werden geënquêteerd, laat zien dat het merendeel van de organisaties aangeeft niet volledig in control te zijn ten aanzien van autorisaties ([KPMG06]). Zo geeft het merendeel van de geënquêteerden aan niet te weten of de uitgegeven autorisaties correct zijn en geen goed en up-to-date-overzicht te hebben van de verstrekte autorisaties. Wetende dat controleerbaarheid en het uitvoeren van deze controles één van de belangrijkste vereisten is van eerdergenoemde diverse wet- en regelgeving, is het niet erg bemoedigend dat slechts 38 procent van de geënquêteerden regelmatig autorisaties controleert.

Autorisatiemanagement – relatie met compliance

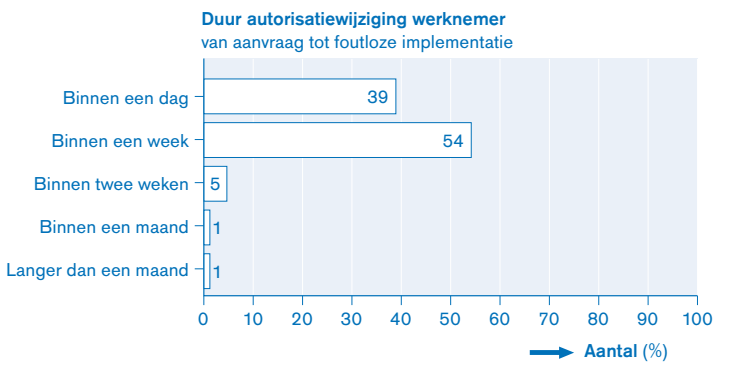
Met de komst van SOX, Basel II en Tabaksblat is transparantie een niet te ontwijken eis geworden voor veel organisaties. In tabel 1 wordt een overzicht gegeven van de meest in het oog springende wet- en regelgeving. Het merendeel hiervan stelt ten aanzien van privacy en integriteit van data soortgelijke vereisten. Deze vereisten zijn terug te voeren op richtlijnen voor de opzet van autorisatiemodellen binnen organisaties evenals het proces van beheer van toegang tot data. Daarbij is het noodzakelijk om het daadwerkelijk voldoen aan deze vereisten aantoonbaar te maken (compliance). Recent onderzoek van The Ponemom Institute toont aan dat de meeste organisaties een handmatige aanpak hebben voor het verifiëren van controls ten aanzien van autorisaties ([Pone07]).

De meeste wet- en regelgeving behandelt:
- privacy- en data-integriteit;
- het beheer van toegang tot deze data ('wie heeft toegang tot welke data en hoe wordt dit gegarandeerd');
- een verandering van 'vertrouwen' naar 'bewijzen' → aantoonbaar 'in control' zijn.

Kortom, indien een organisatie niet aantoonbaar 'in control' is, bestaat er dan een oplossing waarbij een organisatie op een efficiënte wijze effectief autorisatiemanagement kan inrichten?

In de voorgaande paragraaf is aangegeven dat veel organisaties niet 'in control' zijn ten aanzien van autorisatiemanagement. Veel organisaties starten projecten, of hebben reeds projecten gestart, om het autorisatiemanagement te verbeteren. Uit al gestarte projecten blijkt dat veel organisaties moeite hebben met de tijdige realisatie van hun doelstelling, te weten effectief en efficiënt autorisatiemanagement. Belangrijke oorzaken hiervan zijn:

- 73% van de ondervraagden weet niet of uitgegeven autorisaties correct zijn.
- 77% van de ondervraagden heeft geen goed up-to-date inzicht in de verstrekte autorisaties.
- Slechts 38% van de ondervraagden geeft aan autorisaties regelmatig te controleren.

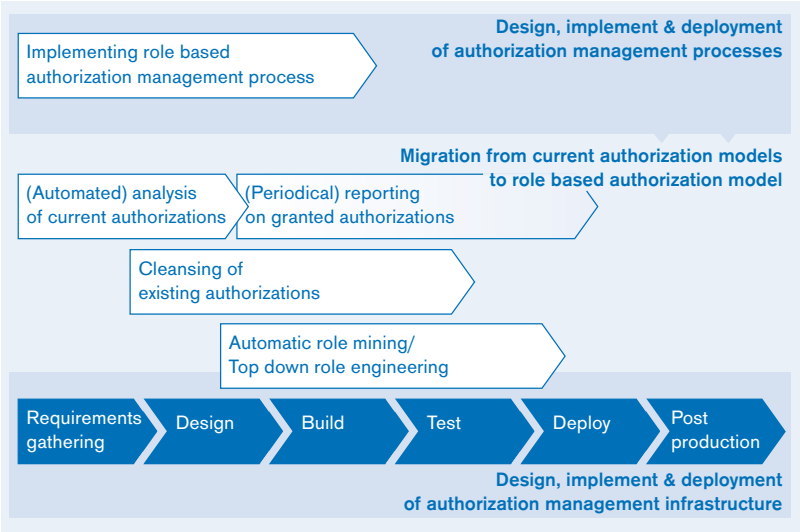


Kader 1. Enkele uitkomsten enquête KPMG ten aanzien van autorisaties.

- Geen gefaseerde aanpak met tussenresultaten. Wanneer een organisatie direct een zeer fijnmazig rollenmodel wil implementeren, kost dit een behoorlijke inspanning wat een langdurig traject tot gevolg heeft. Het risico hiervan is dat projecten worden gestaakt omdat na verloop van tijd nog steeds geen concrete resultaten zijn geboekt en de organisatie nog niet 'in control' is.
- Veel projecten worden vanuit de IT-organisatie opgestart, waardoor de aansluiting met de business niet of nauwelijks wordt bereikt.

Risk Management	
Legislation	**Description**
• USA PATRIOT Act	Enacts 'Know Your Customer' anti-money laundering regulations
• Sarbanes Oxley	Sets higher financial reporting and governance standards for corporate boards and executives
• KonTrag (Germany)	Requires directors to establish risk management supervisory systems and report 'control' information to shareholders
• Gramm-Leach Bliley	Requires financial institutions to safeguard and keep private 'non-public' consumer information
• HIPAA	Requires health care institutions to safeguard and keep private 'individually identifiable patient health information'
• UK Combined Code	
• Basel II	New draft accord requires financial institutions to report on 'operational risk'
• SEC White Paper	SEC/OCC/Fed draft regulations sets new standards for data center proximity and industry testing

Tabel 1. Overzicht van toepasselijke wet- en regelgeving.

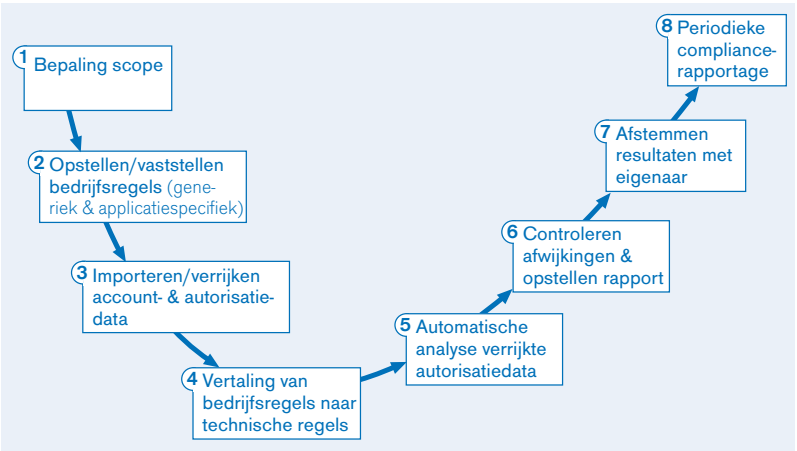


Figuur 1. Aanpak verbetering van autorisatiemanagement.

- Het autorisatiemanagementproces wordt niet verbeterd en uitgebreid in relatie tot het beheren van rollen, een middel waarmee de organisatie in staat wordt gesteld haar verantwoordelijkheid te nemen ten aanzien van autorisatiemanagement.

Om wel tot een succesvol project te komen en de organisatie 'in control' te brengen ten aanzien van autorisatiemanagement moet de projectaanpak:
- efficiënt en pragmatisch zijn. De business moet worden betrokken maar de benodigde betrokkenheid van de business, uitgedrukt in tijd, moet minimaal zijn. Zo niet, dan verliest het project al snel draagvlak.
- leiden tot een structurele oplossing zodat er niet ieder jaar een opschoningstraject hoeft te worden gestart.
- snel resultaat opleveren zodat de grootste problemen snel worden opgelost en het project aantoont echt toegevoegde waarde te bieden.

In figuur 1 is de aanpak waarmee autorisatiemanagement wordt verbeterd, schematisch weergegeven.



Figuur 2. Compliance-verificatieproces ten aanzien van autorisatiemanagement.

Belangrijkste onderdelen hieruit zijn:
- het inrichten van een complianceverificatieproces teneinde snel het eerste niveau van compliance te bereiken. In dit proces wordt gerapporteerd over de status van de huidige uitgegeven autorisaties en het management neemt mitigerende acties op basis van de rapportages.
- het herinrichten, optimaliseren en automatiseren van delen van het autorisatiemanagementproces om nieuwe vervuiling te voorkomen en om te kunnen werken met rolgebaseerde autorisaties. Hierbij wordt het gebruik van een autorisatiemanagementtool aangeraden.

Het complianceverificatieproces

Het inrichten van het complianceverificatieproces

Aangezien het aantonen van het niveau van compliance voor de organisatie vaak de hoogste prioriteit heeft, richt de eerste stap zich dan ook op het opzetten en inrichten van dit verificatie- en rapportageproces. In dit proces wordt in kaart gebracht welke bedrijfsregels er gelden ten aanzien van autorisaties (bijvoorbeeld functiescheiding) en wordt gevalideerd of de regels in de praktijk ook zijn nageleefd bij de daadwerkelijk geïmplementeerde autorisaties. De uitvoering van deze stap is daarnaast noodzakelijk om autorisaties rolgebaseerd te kunnen gaan beheren. Anders gaat men immers foutieve autorisaties in nieuwe rollen opnemen.

De zogenoemde bedrijfsregels worden afgeleid van intern beleid en procedures, evenals externe wet- en regelgeving, zoals:
- SOX 404;
- mededingingswetgeving (NMa);
- privacywetgeving (Wet bescherming persoonsgegevens).

De bedrijfsregels worden opgesplitst in generieke en applicatiespecifieke regels. De generieke regels zijn van toepassing op de autorisaties van alle applicaties. Daarnaast kunnen ook generieke regels bestaan voor het beheer van de IT-infrastructuur. Naast de generieke regels wordt per applicatie bepaald welke regels van toepassing zijn in relatie tot de autorisaties. Deze specifieke regels worden vaak opgesteld op basis van beschikbare functionele ontwerpen, risicoanalyses in relatie tot functiescheiding en beschikbare autorisatiematrices. Tabel 2 geeft een aantal voorbeelden van bedrijfsregels.

Om een efficiënte analyse mogelijk te maken, kan voor complianceverificatie een geautomatiseerde analysetool worden gebruikt. Het voordeel hiervan is dat de analyse vele malen sneller wordt uitgevoerd. Eigenlijk is een handmatige analyse onmogelijk voor omvangrijke applicaties en gebruikersgroepen. Een tweede voordeel is, dat de analyse consistent wordt uitgevoerd op basis van geprogrammeerde regels.

Het is hierbij belangrijk om zich te realiseren dat de analysetool slechts een hulpmiddel is. Er moet nog steeds een proces worden ingericht en het opstellen van de bedrijfsregels is iets wat een analysetool niet doet. De inhoud van de bedrijfsregels bepaalt de output van de analyse en niet een geavanceerde analysetool die mogelijk door ondeskundigen wordt gebruikt.

In figuur 2 is het complianceverificatieproces schematisch weergegeven en in tabel 3 is iedere processtap kort beschreven.

Resultaat van het complianceverificatieproces

Het beschreven complianceverificatieproces stelt de organisatie in staat:
- op een snelle wijze te rapporteren over het niveau van compliance ten aanzien van voor de organisatie geldende compliancevereisten ten aanzien van autorisatiemanagement;
- de verantwoordelijkheid bij de juiste functionarissen te beleggen;
- door het verkregen inzicht de gewenste situatie ten aanzien van autorisaties te herstellen door het opschonen van accounts en autorisaties (verwijderen van zogenaamde 'ghost accounts' en van excessieve toegangsrechten);
- op basis van de opgeschoonde situatie haar autorisatiemanagement structureel te verbeteren en desgewenst rolgebaseerd autorisatiemanagement in te voeren.

Generieke maatregelen	Applicatiespecifieke maatregelen
• Individuele aansprakelijkheid (autorisaties toegekend aan specifieke individuele gebruikers; gebruikersidentiteiten worden niet gedeeld)	• Autorisaties beperken tot gepaste functionele organisatorische scope en processen (indien noodzakelijk met 'Chinese Muren' als gevolg)
• Een gebruikersidentiteit per gebruiker (per platform per gebruiker enkele identiteit)	• Autorisaties op hoog niveau scheiden tussen productie-, acceptatie/test- en ontwikkelomgevingen
• Autorisaties toekennen met rollen of gelijkwaardige groepeermechanismen • Directe koppelingen tussen gebruikers en bronnen vermijden	• Autorisaties laten overeenkomen met vereiste functiescheidingen (combinaties van bepaalde autorisaties niet toegestaan)
• Geen gebruiker bezit alle autorisaties • Geen gebruiker bezit zo veel autorisaties dat risico op (on)bewust misbruik groot wordt	• Specifieke autorisaties bij specifieke functies (bijv. alleen leesrechten voor auditors)
• Geen 'orphan accounts' op platform en/of toepassing	
• Verlopen gebruikers/autorisaties scheiden van actieve set (organisatie kan die om bepaalde redenen aanhouden)	

Tabel 2. Voorbeelden van generieke en applicatiespecifieke maatregelen.

Stap	Omschrijving
① Bepaling scope	• Eerste activiteit complianceverificatieproces is vaststellen van scope ten aanzien van: – toepassingen en systemen – vaststelling eigenaren toepassingen en systemen – geldende beleidsuitgangspunten
② Opstellen/vaststellen bedrijfsregels, zowel generiek als applicatiespecifiek	• Generieke bedrijfsregels voor bedrijfsapplicaties & IT-infrastructuur worden verkregen op basis van analyse van het informatiebeveiligingsbeleid en andere relevante beleidsdocumenten & beschikbare 'good practices'. Ook worden interviews afgenomen met bijvoorbeeld de security officer en de voor IT-infrastructuur verantwoordelijke persoon • Om specifieke bedrijfsregels te verzamelen worden interviews afgenomen met de proces- & applicatie-eigenaren en de functioneel beheerders van bedrijfsapplicaties. Doel is om informatie te verzamelen over de door de bedrijfsregels ondersteunde processen en het autorisatieconcept, evenals de huidige toegepaste controles bij autorisatiebeheer, zoals van toepassing zijnde functiescheidingsvereisten
③ Importeren/verrijken account- & autorisatiedata	• Autorisatiedata worden ingelezen in analysetool en verrijkt met hr-data, zodat automatische analyse kan worden uitgevoerd (voor een aantal controles kan niet worden volstaan met 'platte' autorisatiedata voorhanden in de toepassing of het systeem); bijv. controle of ieder account herleidbaar is tot enkel individu uit hr-administratie • In figuur 2 is de samenhang tussen de stappen en het gebruik van de tool schematisch weergegeven
④ Vertalen van bedrijfsregels naar technische regels	• Voor de geautomatiseerde analyse worden bedrijfsregels vertaald naar technische regels in de analysetool
⑤ Automatische analyse verrijkte autorisatiedata	• Op grond van technische regels en ingelezen data wordt de automatische analyse uitgevoerd
⑥ Controleren afwijkingen & opstellen rapport	• Verificatie of bedrijfsregels juist zijn geconverteerd naar technische regels waarna resultaten worden afgestemd met applicatie- & proceseigenaren
⑦ Afstemmen resultaten met eigenaar	• Op grond van rapporten (stap 6) worden analyseresultaten met betrokkenen besproken om te bepalen of bedrijfsregels moeten worden aangepast of dat geïmplementeerde autorisaties moeten worden aangepast op basis van afwijkingen
⑧ Periodieke compliancerapportage	• Met analyses op grond van meest actuele autorisatie- en hr-data wordt vastgesteld of de opgestelde compliancedrivers en de technische vertaling in de zogenaamde Business Process Rules correct zijn (deze worden gebruikt tijdens de periodieke compliancerapportage)

Tabel 3. Processtappen behorende bij complianceverificatie.

Aandachtspunten bij de inrichting van het complianceverificatieproces

Bij de inrichting van het complianceverificatieproces spelen de volgende aandachtspunten c.q. randvoorwaarden een belangrijke rol:
- Van de applicaties in scope moet een eigenaar bekend zijn en tevens moet functioneel en technisch beheer helder zijn belegd. Deze betrokkenen moeten immers de benodigde documentatie en informatie aanleveren.
- Beschikbaarheid van up-to-date documentatie zoals beleidsuitgangspunten ten aanzien van autorisatiemanagement, evenals autorisatiematrices en systeemdocumentatie waarin ook het autorisatiemodel van de applicatie wordt beschreven.
- Beschikbaarstelling van de data, zeker als het systeem of de toepassing is geoutsourcet. Vaak zijn hierover geen afspraken gemaakt in de contracten of service level agreements (SLA).
- Veel controles maken gebruik van verrijkte data. Het moet dus mogelijk zijn de 'platte' autorisatiedata uit een systeem of toepassing te verrijken met hr-data. Ofwel de gebruikersidentiteit moet herleidbaar zijn tot een natuurlijk persoon in hr.
- Het autorisatieconcept van de toepassing zelf. Maakt de applicatie bijvoorbeeld gebruik van Active Directory-groepen voor de autorisatie of werkt de applicatie met een eigen autorisatiedatabase?

Is uw organisatie 'in control' na complianceverificatie?

In principe wel, want de autorisaties zijn nu weer op orde. Om 'in control' te blijven is het echter een randvoorwaarde dat de autorisatiemanagementprocessen (aanvraag, goedkeuring, controle) goed zijn ingericht. En dit is nu juist de uitdaging, het complianceverificatieproject is immers niet voor niets gestart. Gedurende het opschonen is het dus van belang dat het autorisatiemanagementproces wordt verbeterd. Dat kan natuurlijk op een procedurele wijze, met daarbij onderstaande nadelen:
- grote beheerinspanning;
- risico op verslappen van aandacht voor autorisaties;
- controle achteraf en dan in het bijzonder ten aanzien van de aangebrachte autorisaties, echter geen controle op het totstandkomingsproces (autorisatiemanagementproces).

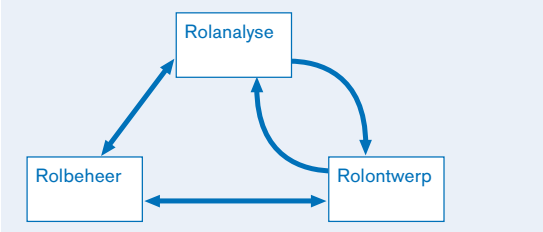
Om dus 'in control' te blijven is een structurele oplossing nodig die zich richt op:
1. Herinrichting van autorisatiemanagement op basis van rolgebaseerd autoriseren. Hierbij komen de volgende aspecten aan bod:
   - rolanalyse;
   - rolontwerp;
   - rolmanagement.
2. Automatiseren van delen van de autorisatiemanagementprocessen. Hierbij ligt een nauwe relatie met het thema Identity & Access Management (IAM). Het verband tussen autorisatiemanagement en IAM wordt aan het slot van dit artikel behandeld.

Herinrichting van autorisatiemanagement, met als uitgangspunt rolgebaseerd autoriseren

Essentie van rolgebaseerd autoriseren is dat een gebruiker geautoriseerd wordt voor toegang tot een object via één of meer rollen. De voordelen van rolgebaseerd autoriseren worden in detail weergegeven in kader 2 verderop in dit artikel.

De levenscyclus van rollen

Een rol is allesbehalve statisch te noemen. Aangezien een organisatie en haar 'business' aan verandering onderhevig zijn, geldt dit ook voor autorisaties en bijbehorende rollen. Hierbij is het van belang te zoeken naar een goede balans tussen hoeveelheid rollen en benodigde rolwijzigingen. Om een dergelijk proces goed in te kunnen richten, is het om te beginnen belangrijk de levenscyclus van rollen te onderkennen. Deze wordt weergegeven in figuur 3.

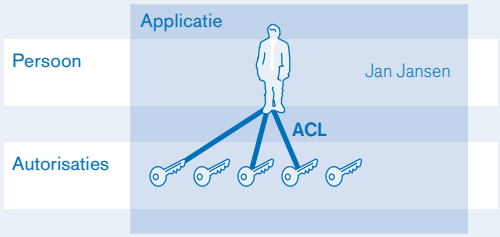


Figuur 3. Levenscyclus van rollen.

De levenscyclus van rollen bevat drie fasen:
- *Rolanalyse*. Tijdens de rolanalyse worden de rollen geïdentificeerd die binnen de organisatie kunnen worden onderkend. De rollen worden geïdentificeerd op basis van onder meer beleidsdocumenten, de organisatiestructuur, bedrijfsprocessen en functieomschrijvingen.
- *Rolontwerp*. Tijdens het rolontwerp worden de rollen geïdentificeerd zoals deze zijn geïmplementeerd in de geautomatiseerde systemen. Op basis van de rolanalyse en het onderzoek naar de rollen in de geautomatiseerde systemen wordt een nieuw ontwerp voor rollen ontwikkeld, dat wordt vastgelegd in een zogenoemde rolcatalogus.
- *Rolmanagement*. Rolmanagement omvat de processen voor het management van rollen, zoals aanvraag, aanmaak, activering, intrekking en schorsing alsmede het doorvoeren van wijzigingen in rollen als gevolg van bijvoorbeeld wijziging van organisatiestructuren, wet- en regelgeving of IT-omgeving.

Traditioneel autorisatiemanagement

Van oudsher heeft elk IT-systeem en elke applicatie een eigen implementatie voor autorisatiemanagement of, preciezer, toegangscontrole. Dit komt erop neer dat een gebruiker gescheiden accounts heeft op elk systeem dat en elke applicatie die hij gebruikt, elk met hun eigen permissiestructuur en methode om autorisaties toe te wijzen.
Over het algemeen zijn de permissiestructuur en de methode om rechten toe te wijzen in deze traditionele systemen vrij direct ingericht. Een veelgebruikte methode voor autoriseren is een Access Control List (ACL). Autorisaties voor de applicaties en systemen zijn direct gekoppeld aan gebruikers of gebruikersgroepen, zoals is weergegeven in de onderstaande afbeelding.

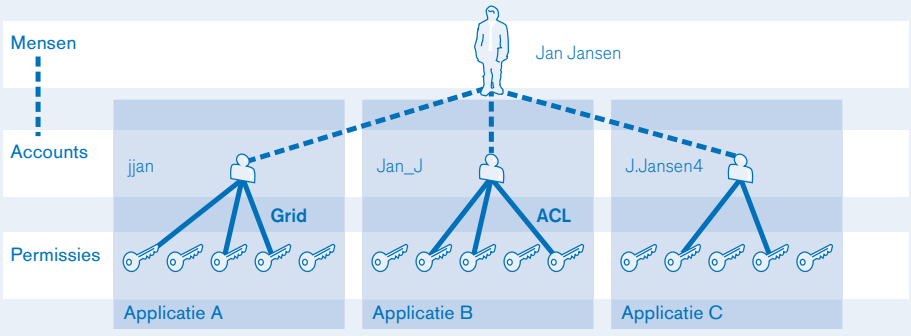


De permissies die gebruikt worden binnen een applicatie of systeem zijn veelal op een gedetailleerd en technisch niveau.
De (bijna) directe relatie tussen de technische autorisaties en de gebruikers maakt dat het moeilijk is om op een functioneel niveau snel te zien wat een gebruiker daadwerkelijk binnen het systeem of de applicatie kan doen. Hieruit volgt dat het zeer lastig is om de toegang voor gebruikers te beheren.

Het gebrek aan overzicht van de toegangsrechten en de mogelijkheid tot goed beheer van deze rechten binnen organisaties neemt toe met het aantal systemen en applicaties dat in gebruik is. Naast het feit dat het gebruik van meerdere applicaties betekent dat het aantal permissies toeneemt en het aantal toewijzingsmethoden dat begrepen en geanalyseerd moet worden groter wordt, gaat het bestaan van meerdere accounts per gebruiker ook een rol spelen.
Verschillende systemen hebben verschillende regels, beperkingen of simpelweg ander beleid voor het aanmaken van accountnamen, wat betekent dat een gebruiker bij verschillende systemen bekend is onder verschillende accounts. Deze situatie wordt in de figuur onderaan weergegeven.

De volgende stappen moeten worden ondernomen om een overzicht te krijgen van de rechten die een gebruiker heeft op de IT-resources van een organisatie:
- Stel vast welke accounts een gebruiker heeft op alle systemen waar hij toegangsrechten bezit. Dit kan een 'kip en ei'-probleem opleveren, omdat een gebruiker over het algemeen toegang heeft tot systemen waarop hij een account heeft.
- Bepaal welke (technische) permissies de gebruiker heeft binnen elk systeem, gebruikmakend van alle gebruikersaccounts.
- Onderzoek wat de gebruiker op functioneel (business) niveau daadwerkelijk kan doen met de permissies die hij bezit.

Het doorlopen van deze stappen kan een behoorlijke uitdaging zijn. Het beheren van toegang (door de bovenstaande stappen in omgekeerde volgorde te behandelen) is nog lastiger.



Kader 1. Traditioneel autorisatiemanagement.

Rolanalyse en -ontwerp

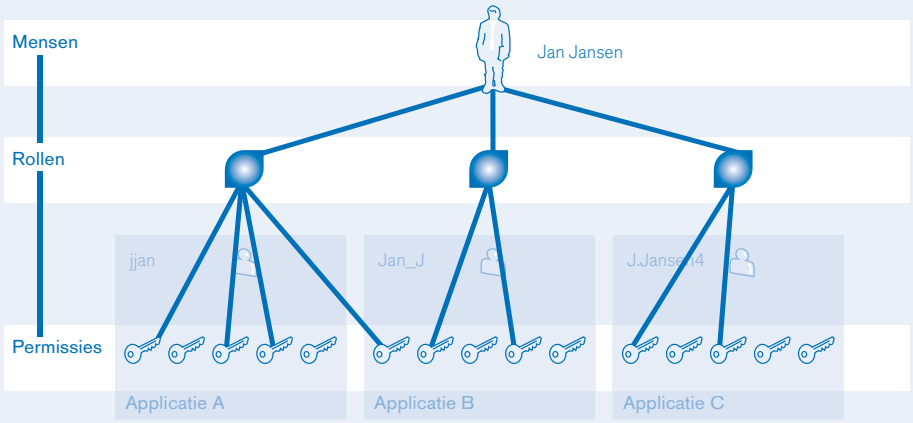
Om te komen van een bestaand autorisatiemodel naar een op rollen gebaseerd autorisatiemodel zijn twee aanpakken mogelijk, te weten ([Mien05]):
- *Top-down rolontwerp*, een veelal meer strategisch georiënteerde aanpak. Hierbij wordt vanuit informatiebeleid, IT-governance en bijbehorende processen (ofwel de administratieve organisatie) bepaald welke autorisaties bij welke rollen zouden moeten horen. Uitdaging hierbij is dat IT-governance in de praktijk eveneens sterk in ontwikkeling is en nog tijd nodig heeft om tot volle wasdom te komen door alle veranderingen die het in ontwikkeling zijn met zich meebrengt.
- *Bottom-up rolontwerp*, een veelal meer operationeel georiënteerde aanpak. Hierbij worden op basis van

Rolgebaseerd autorisatiemanagement (Role Based Access Control)

Zoals de naam doet vermoeden, spelen rollen een belangrijke rol binnen Role Based Access Control (RBAC). RBAC-rollen bevinden zich tussen de permissies en de gebruikers, en hebben zowel een functie bij het organiseren als bij het koppelen van deze niveaus. Dit wordt onder in dit kader afgebeeld.

Binnen dit model is een permissie een recht om een zekere actie op een bepaald (type) object te voltooien. De permissies zijn samengevoegd in rollen. De rollen worden toegewezen aan gebruikers. Zodra dit gebeurt, zijn de permissies binnen die rol ook beschikbaar voor de gebruiker.
Hoewel rollen slechts een kleine toevoeging lijken te zijn aan de traditionele autorisatiemanagementoplossingen, zijn ze wel degelijk een belangrijke factor in het verplaatsen van autorisatiemanagement naar het businessniveau. Een aantal redenen is hiervoor te geven, waaronder:

- Een enkele rol kan permissies voor meerdere systemen of applicaties bevatten. Rollen overstijgen daardoor de grenzen van die systemen en applicaties. In traditionele autorisatiemanagementoplossingen compliceren deze grenzen het verkrijgen van een overzicht van en grip op permissies van gebruikers.
- Aan rollen kunnen namen worden gegeven die betekenisvol zijn voor de business, en rollen zijn op deze manier ook te relateren aan businessconcepten. Bijvoorbeeld, als bepaalde permissies worden toegekend aan medewerkers met een bepaalde functie binnen de organisatie, dan kunnen die permissies worden gegroepeerd in een rol die de naam draagt van die functie. De permissies worden dan toegekend aan de betrokken medewerkers in die functie door hen die rol te geven. Ook mogelijk is dat sommige permissies toegekend worden aan alle medewerkers. In een dergelijk geval kan er een rol worden gemaakt met de naam 'Medewerker' die wordt toegekend aan alle medewerkers.
  Het kunnen geven van betekenisvolle namen aan rollen is een belangrijk voordeel. Immers in de huidige situatie wordt het verantwoordelijke management vaak geconfronteerd met allerlei technische benamingen van autorisatieprofielen, welke voor hem eigenlijk geen betekenis hebben. Hierdoor kan hij geen verantwoordelijkheid nemen ten aanzien van autorisatiemanagement.
- Rollen ondersteunen situaties met meerdere abstractieniveaus van permissies door gebruik te maken van rolovererving. Door rolovererving kunnen rollen die permissies bevatten zelf ook gecombineerd worden tot abstractere rollen.
  Stel bijvoorbeeld dat een organisatie applicatie-eigenaren heeft die over gedetailleerde kennis beschikken van de technische permissies binnen hun applicaties. Deze applicatie-eigenaren kunnen deze technische permissies groeperen in rollen, waarbij elke rol de permissies bevat die nodig zijn om een bepaalde taak binnen de applicatie uit te voeren. Een lijnmanager kan deze applicatierollen combineren, om zo tot rollen op een hoger niveau te komen. Elk van deze laatste rollen kan overeenkomen met een businessfunctie.
- Rollen vormen een basis voor het implementeren van bepaalde beleidsregels, zoals functiescheidingen. Een beleidsregel die stelt dat twee taken of functies niet toegekend mogen worden aan dezelfde werknemer, kan vertaald worden naar een RBAC-regel die ervoor zorgt dat de betrokken rollen niet aan dezelfde gebruiker worden toegekend.



Kader 2. Rolgebaseerd autorisatiemanagement.

bestaande autorisaties binnen geselecteerde objecten op een geautomatiseerde wijze rollen gedestilleerd. Hiertoe zijn reeds diverse tools beschikbaar, alhoewel de markt van dergelijke tools nog erg in ontwikkeling is. Een uitdaging hierbij is daarom vooral het vertalen van de uitkomsten van deze technische analyse naar voor objecteigenaren begrijpelijke uitkomsten.

In werkelijkheid zullen deze aanpakken worden gecombineerd, waarbij bottom-up rolengineering zal worden

uitgevoerd met gebruik van geautomatiseerde tools, waarna deze IT-rollen gecombineerd zullen worden tot businessrollen met gebruik van de top-downaanpak.

Om te kunnen beginnen met het bottom-up rolontwerp met gebruikmaking van geautomatiseerde rapportages en analysetools, is het nodig dat de data die zullen worden geanalyseerd bij het rolminingproces voldoen aan bepaalde kwaliteitscriteria. Gebaseerd op zowel de eerste analyse van de datakwaliteit als de rapporten over de verleende permissies naar de betrokken stakeholders worden de bestaande autorisaties geschoond. Na het bereiken van het benodigde kwaliteitsniveau wordt het geautomatiseerde rolminingproces gestart, gecombineerd met de top-down rolengineering van de resultaten uit de stap waarbij de rolminingactiviteiten worden omgezet naar businessrollen.

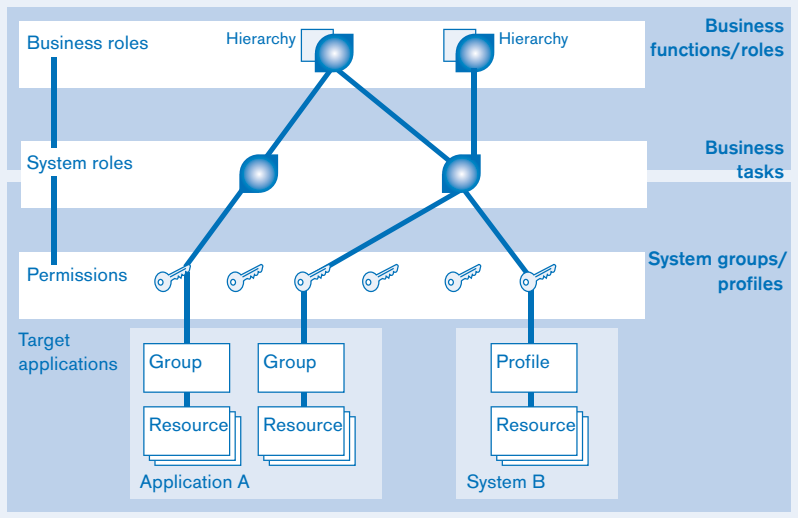
Nadat deze schoningsactiviteiten hebben geleid tot autorisatiedata van het vereiste kwaliteitsniveau, kan het proces van rolmining en rolengineering van start gaan. Rolmining wordt gebruikt voor het ontdekken van IT- of systeemrollen en rolengineering wordt gebruikt voor het creëren van businessrollen (ofwel het combineren van IT- of systeemrollen tot betekenisvolle businessrollen).

Het verschil tussen businessrollen en IT- of systeemrollen wordt weergegeven in figuur 4.

In autorisatiemanagement maken we een onderscheid tussen:
- *Permissieniveau*. Dit is het laagste en meest grove niveau binnen de autorisatiemanagementaanpak. De permissies van deze aanpak zijn gekoppeld aan groepen, profielen of gelijkwaardige gebruikerscontainers in de beheerde applicaties.
- *IT- of systeemrollen*. Bevatten veelal permissies die nodig zijn om een bepaalde businesstaak uit te voeren. Bedenk dat IT- of systeemrollen permissies kunnen bevatten van één of meer applicaties.
- *Businessrollen*. Komen overeen met businessfuncties of zelfs businessrollen, en worden gecreëerd door het combineren van de daarvoor benodigde systeemrollen (de businesstaken).

Opgemerkt moet worden dat het mogelijk is meerdere niveaus van de zojuist genoemde businessrollen toe te voegen. Op deze manier wordt een businessrolhiërarchie gecreëerd. In de praktijk is het aantal omgevingen waarin dit noodzakelijk of praktisch is, vrij beperkt.

Met betrekking tot de autorisatiemanagementaanpak kunnen de volgende taken worden geïdentificeerd:
1. Rolmining met behulp van een geautomatiseerde rolminingtool:
   – het identificeren en creëren van permissies;
   – het samenstellen van systeemrollen.
2. Het samenstellen van businessrollen via een top-downaanpak.



Figuur 4. Verschil tussen businessrollen en systeemrollen.

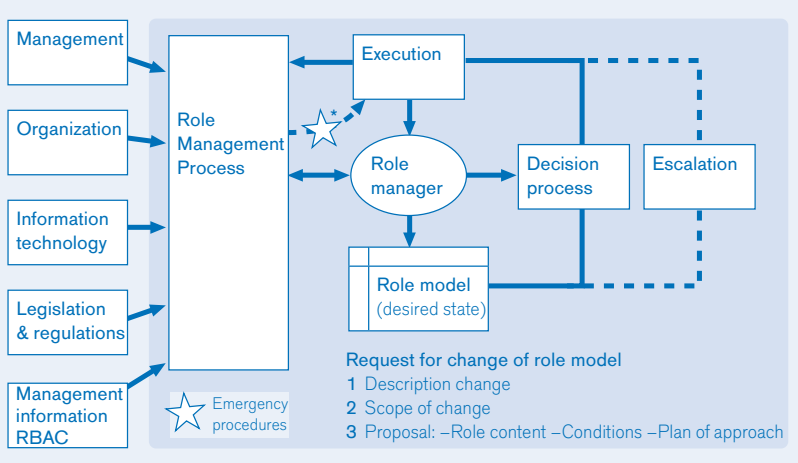
3. Het implementeren en toepassen van beleidsregels (zoals functiescheidingen en rolactivatie gebaseerd op zogenaamde 'rules'). Deze regels kunnen per rol worden aangegeven.

Rolmanagement

Een rol is een generieke term voor het groeperen van toegangsrechten die benodigd zijn voor het uitvoeren van taken door de gebruiker. In veel gevallen zijn deze taken direct gerelateerd aan de activiteiten die deze persoon uitvoert in een proces, een project of zijn of haar organisatorische eenheid.
Om te garanderen dat het ontwikkelen en managen van rollen volgens een consistent en uniform proces verloopt, is het belangrijk om rolmanagement in de organisatie te verankeren.

Rolmanagement bevat wijzigingsbeheer voor de roldefinities, gebaseerd op het managementbeleid. De coördinator van dit proces is de tactische rolmanager. De rol van de tactische rolmanager en de betrokken partijen en processen zijn getoond in figuur 5.

Figuur 5. Overzicht tactisch rolmanagement.



Rolmanagement				
Doel	**Verantwoordelijk** (Responsible)	**Aansprakelijk** (Accountable)	**Raadpleeg** (Consult)	**Informeer** (Inform)
Rolmanagement	Functioneel management	Risk manager	• Lijnmanager • Systeem-/applicatie-eigenaar • Risk manager	• Systeem-/applicatie-eigenaar • Risk manager

Tabel 4. RACI-matrix behorend bij rolmanagement.

Het proces van het toewijzen van rollen aan gebruikers maakt geen deel uit van rolmanagement.

De uitkomst van het rolmanagementproces bestaat uit de definitie van de rollen. Deze definities kunnen worden opgeslagen in de autorisatiemanagementinfrastructuur.

Het beleid voor rolmanagement bevat met name een beschrijving van hoe de governancestructuur moet zijn met daarbij diverse rollen en verantwoordelijkheden van de betrokken functionarissen. Hierbij kan een zogenaamd RACI-schema worden gehanteerd (zie tabel 4).

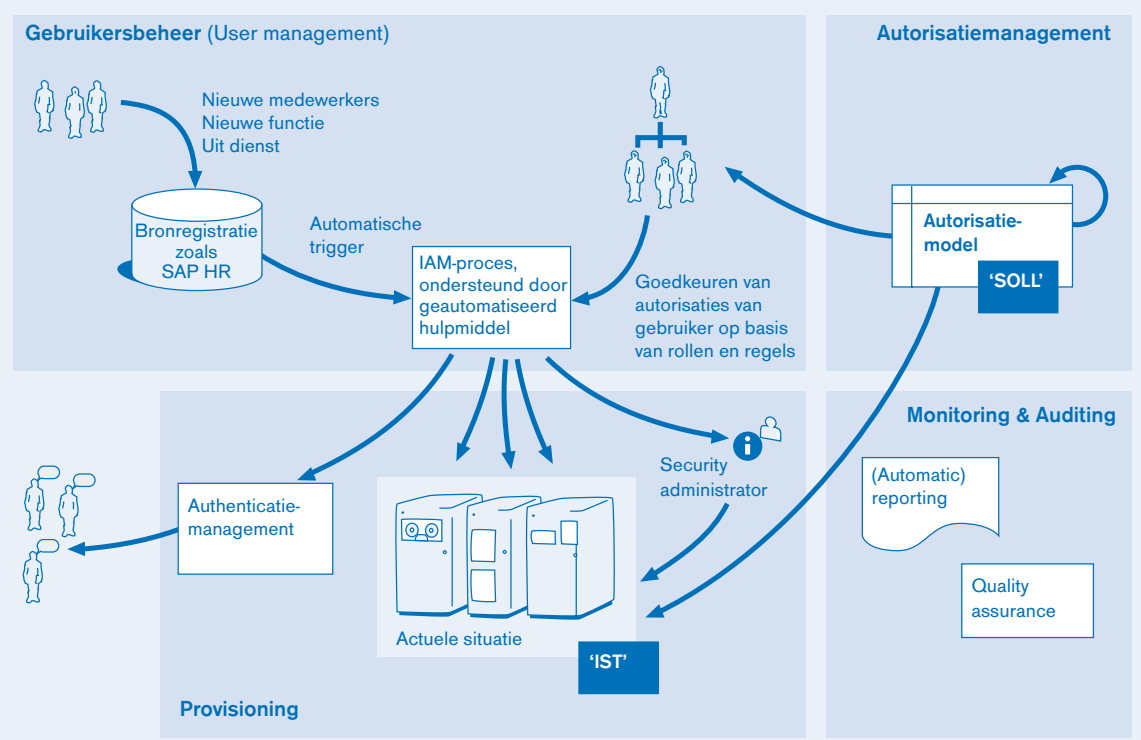
Automatiseren van delen van de autorisatiemanagementprocessen

Teneinde een te onderhouden autorisatiemodel gebaseerd op rollen te verkrijgen, verdient het de voorkeur om de uitkomsten van rolanalyse en -ontwerp vast te leggen in een daarvoor ontworpen geautomatiseerd systeem. Hier geldt de anekdote 'boekhouding kun je natuurlijk op papier doen, met een geautomatiseerd systeem is het toch wel wat efficiënter'.

Naast dat enerzijds de roldefinities zullen worden vastgelegd in een geautomatiseerde administratie, zullen daarin anderzijds ook aspecten worden opgenomen als welke groep functionarissen welke rollen mag toedelen, alsmede condities en voorwaarden waaronder een rol mag worden toebedeeld.

Rolgebaseerd autorisatiemanagement en IAM

In [Herm06] wordt een toelichting gegeven op een integrale set van processen die tezamen IAM wordt genoemd. Naast autorisatiemanagement, dat in dit artikel centraal staat, bestaat IAM uit een viertal andere processen. In figuur 6 worden deze (nogmaals) weergegeven. Naast de drijfveer 'compliance' en dientengevolge benodigde 'verification' is algehele procesverbetering ('operational excellence') een nimmer verdwijnend thema binnen organisaties. Het valt dan ook aan te bevelen om de inspanningen rondom autorisatiemanagement hand in hand te laten gaan met verbeteringen in de andere IAM-processen. Zo kunnen bijvoorbeeld aanvraagprocessen voor autorisaties alsmede het doorzetten van gewenste autorisaties (provisioning) richting objecten



Figuur 6. Overzicht IAM-processen.

Resultaat van de herinrichting van autorisatiemanagement

- Er is altijd een up-to-date inzicht in de autorisaties van medewerkers.
- Een efficiënte en effectieve migratie naar het rolgebaseerd autorisatiemodel.
- De huidige gewenste situatie is vastgelegd in het autorisatiesysteem.
- De huidige situatie komt overeen met de gewenste situatie.
- De efficiëntie kan worden verhoogd door gebruik te maken van analytische tools.
- De transparantie, het onderhouden, de effectiviteit en de verificatiemogelijkheden worden verbeterd.
- Autorisatiemanagement is aantoonbaar 'in control'.
- Door autorisatiemanagement nadrukkelijk in verband te brengen met (bestaande) inspanningen op het gebied van IAM kan er verdere 'operational excellence' worden behaald.

Kader 3. Resultaten van de herinrichting van autorisatiemanagement.

Aandachtspunten bij herinrichting van autorisatiemanagement

Rolmining

- Automatische rolmining heeft alleen succes als de te minen data voldoen aan de vereiste kwaliteitscriteria.

Rolengineering

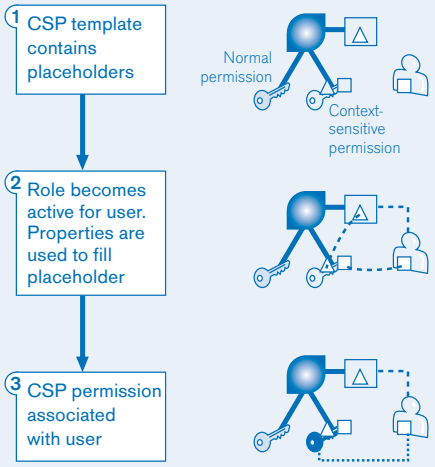
- Te veel variatie in rollen – de implementatie van een autorisatiemodel dat gebaseerd is op rollen is bedoeld om het aantal administratieactiviteiten te verkleinen door te standaardiseren. Om het aantal (variaties in) rollen te beperken, is het mogelijk contextafhankelijkheid onderdeel te laten uitmaken van het rolontwerp.
- Een mogelijk probleem dat vaak wordt genoemd in relatie tot de implementatie van RBAC-oplossingen is rolexplosie of rolproliferatie. Rolexplosie kan voorkomen in een situatie waarbij een zeer groot en vrijwel onbeheersbaar aantal rollen moet worden gemaakt om alle permissies in de IT-omgeving te omvatten. Een nadere analyse van de oorzaken die hieraan ten grondslag liggen geeft vaak weer dat meestal te veel op elkaar lijkende permissies in gebruik zijn; ook wel omschreven als permissie-explosie.
- Normaal gesproken zijn de verschillen tussen permissies min of meer direct te relateren aan de context waarin ze gebruikt worden. Bijvoorbeeld, in een organisatie waarin iedere divisie haar eigen fileshare op het netwerk heeft, moet men vaak een aparte permissie aanmaken voor iedere fileshare, en dus voor elke divisie. Bovendien is het nodig om een aparte rol voor elke divisie aan te maken die de filesharepermissie voor de divisie in kwestie bevat.
- Soortgelijke voorbeelden kunnen worden gegeven voor organisaties (of divisies) met meerdere geografische locaties, medewerkers met verschillende niveaus van senioriteit, enz.

Om dit probleem te verhelpen kan het concept van zogenaamde Context-Sensitive Permissions (CSP's) worden overwogen. CSP's kunnen dienen als permissiesjablonen die velden voor contextinformatie kunnen bevatten.

Contextinformatie kan een eigenschap zijn van:

- de applicatie waarvoor de permissie is gedefinieerd;
- de rollen waarin de permissie is gevat;
- de organisatorische eenheid en gebruikers aan wie de rollen worden toegewezen.

Wanneer een CSP daadwerkelijk wordt toegekend aan een gebruiker (door toekenning of activering van een rol die de CSP bevat) wordt de permissie voor die gebruiker aangemaakt door de relevante eigenschappen op te halen en ze te gebruiken om het sjabloon in te vullen. De afbeelding hieronder laat dat zien.



Als de CSP wordt gekoppeld aan een andere gebruiker, wordt mogelijk een verschillende permissie aangemaakt. Dit zou het geval kunnen zijn als de tweede gebruiker lid is van een andere organisatorische eenheid en de CSP velden bevat voor eigenschappen van organisatorische eenheden. Door dit mechanisme is het niet nodig om handmatig meerdere permissies of rollen toe te wijzen om verschillende toegangsrechten toe te kennen.

Dit maakt Context Sensitive Permissions een zeer krachtige tool om rolexplosie tegen te gaan.

Kader 4. Aandachtspunten voor herinrichting van autorisatiemanagement.

worden geautomatiseerd. Deze vorm van procesoptimalisatie wordt door veel organisaties uitgevoerd binnen een specifiek IAM- of algeheel security-verbeteringsprogramma.

Het verdient hierbij aanbeveling om autorisatiemanagement niet alleen in perspectief te zien met gerelateerde processen maar eveneens benodigde verbeteringen stap voor stap te realiseren (evolutie in plaats van revolutie).

Conclusie

Het krijgen en houden van grip op autorisatiemanagement is van belang voor organisaties. Enerzijds vanuit overwegingen te maken vanuit compliancevereisten, anderzijds vanuit het perspectief van het realiseren van procesverbeteringen (efficiëntie en effectiviteit). Het verdient daarom aanbeveling het beheerproces rondom autorisaties stap voor stap te verbeteren door gebruik te maken van het concept 'rolgebaseerd autoriseren'. Voordeel van het complianceperspectief is dat de aantoonbaarheid van wie toegang heeft tot welke data kan worden vergemakkelijkt.

Echter, invoering van rolgebaseerd autoriseren is bepaald geen sinecure. Waar te beginnen? Welke applicaties eerst, welke kunnen wachten? Hoeveel rollen heb ik eigenlijk nodig? Kritieke succesfactor daarom is vooral het bewandelen van 'de weg van geleidelijkheid'. Hierbij dient een strategische aanpak te worden gecombineerd met een meer operationele. Ofwel beleid en IT-governance als kaderstelling versus concreet per applicatie bekijken welke autorisaties zijn er nu eigenlijk toebedeeld aan mensen en horen die autorisaties er wel te zijn?

Ten slotte is het raadzaam autorisatiemanagement te bezien vanuit het bredere raamwerk van IAM-processen. Tezamen zullen deze uw organisatie stap voor stap aantoonbaar 'in control' brengen en houden!

Literatuur

[Herm06] Ing. J.A.M. Hermans RE, drs. D.B. van Ham CISA en drs. J. ter Hart, *Globalisering en de complexiteit van logische toegang: nut en noodzaak van een strategie op het gebied van Identity & Access Management (IAM)*, Compact 2006/3.

[Herm05] Ing. J.A.M. Hermans RE en drs. J. ter Hart, *Identity & Access Management: operational excellence of 'in control'?*, Compact 2005/3.

[Koor04] Drs. ing. R.F. Koorn RE en ing. J.A.M. Hermans RE, *Identity Management: hoe (on)toereikend is het nu en hoe kan het beter?*, Compact 2004/2.

[KPMG06] KPMG IT Advisory, *Onderzoek informatiebeveiliging: zes belangrijke signalen uit de praktijk*, 2006.

[Mien05] Ing. P. Mienes RE, *De (harde) praktijk van role engineering*, Compact 2005/3.

[Pone07] The Ponemon Institute, *Survey on Identity Compliance*, 1 March 2007.