Globalisering en de complexiteit van logische toegang

Nut en noodzaak van een strategie op het gebied van Identity & Access Management (I AM)

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

Wie heeft toegang tot welke informatie en welke zekerheden hebben organisaties hierover? Dit is een fundamentele vraag die we ons al sinds de komst van mainframes stellen. Echter anno 2006, in een wereld die gekenmerkt wordt door 'any place, any time', is deze vraag nog prangender geworden. Hoe dienen steeds internationaler opererende organisaties nu om te gaan met logische toegang en controle hierop? In dit artikel wordt uitgelegd dat het hebben van een strategie op gebied van *Identity & Access Management* onontbeerlijk is. Daarnaast wordt een (theoretisch) denkkader gepresenteerd over de opkomst van een shared service center op dit gebied en welke diensten een dergelijk organisatieonderdeel kan bieden.

Inleiding

Vanuit ICT-perspectief is globalisering allang geen ver-van-mijn-bedshow meer. Wie belt er bijvoorbeeld tegenwoordig nog naar een helpdesk en krijgt een collega van vier deuren verderop aan de lijn? En als je op zakenreis moet, is het ook normaal dat je direct je laptop inplugt en gewoon kunt werken zonder al te veel moeite (conform het Martini-concept 'any place, any time'). En wat te denken van integratie van informatievoorzieningen bij fusies en overnames? Hoe belangrijk is het om zorg te dragen dat in de nieuwe bedrijfssituatie de juiste mensen toegang hebben tot de juiste informatie?

Dergelijke voorbeelden illustreren de toenemende complexiteit op het gebied van gebruikers en autorisatie. Het managen van gebruikers en autorisaties wordt dan ook steeds complexer. Hierdoor neemt de vraag toe naar een oplossing om als organisatie 'in control' te zijn of te blijven wat betreft de vraag wie nu daadwerkelijk toegang heeft (gehad) tot welke informatie. Het is dan ook niet verwonderlijk dat er een steeds grotere behoefte ontstaat aan efficiënt en effectief toegangsbeheer en om dit vanuit een globaliseringsvisie in te steken.

Dit artikel richt zich vanuit het perspectief van globalisering op het nut, de noodzaak en mogelijkheden van een oplossing, te weten *Identity & Access Management (I AM)*. Er wordt een (theoretisch) denkkader gepresenteerd dat aangeeft dat juist nu, in de huidige dynamische omgeving waarin de meeste organisaties zich bevinden, het verstandig is een strategie te hebben op het gebied van 'wie ben je?' en 'wat mag je?'.

Ing. J.A.M. Hermans RE
is senior manager bij KPMG Information Risk Management 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 Information Risk Management 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 Information Risk Management 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

Wat is I AM?

Allereerst is het belangrijk om toe te lichten wat I AM precies inhoudt. I AM is een paraplubegrip voor een veelvoud van termen. In dit artikel hanteren we de volgende definitie ([Herm05]):

I AM is het beleid, de processen en ondersteunende systemen die managen welke gebruikers (personen, applicaties en systemen) toegang verkrijgen tot informatie, ICT-middelen en fysieke resources en wat iedere gebruiker gerechtigd is hiermee te doen.

Kortweg houdt dit in dat het beheer van gebruikers(rechten) in brede zin centraal staat, en daarbij ook centraal wordt gemanaged. Binnen dit kader laat I AM zich vertalen in een serie componenten en bijbehorende processen (zie figuur 1).

User management
Met behulp van de user-managementcomponent wordt de werknemerscyclus van in- en uitdiensttreding, maar worden ook functiewijzigingen volledig beheerd. Hiermee wordt de basis gelegd voor de registratie van de gebruikers van informatie, ICT-middelen en fysieke resources.

Authenticatiemanagement
Wanneer duidelijk is welke gebruikers er zijn, dienen zij geauthenticeerd te kunnen worden. Met behulp van authenticatiemanagement worden elementen als passwords, tokens, etc. beheerd en uitgereikt aan gebruikers. Hiermee wordt bereikt dat de gebruiker ook echt is wie hij zegt dat hij is, en er dus vanuit de organisatie controle is over 'wie ben je?'.

Autorisatiemanagement
Geauthenticeerde gebruikers moeten gekoppeld worden aan bepaalde rechten voor informatie, ICT-middelen en fysieke resources, voordat zij toegang kunnen krijgen tot die objecten. Autorisatiemanagement biedt beheer van die rechten van gebruikers teneinde volledige controle te hebben over 'wat mag je?'.

Provisioning
Uiteindelijk dienen de rechten van gebruikers te worden gerouteerd naar (ICT-)objecten die benaderd worden. Het doorvoeren van de gebruikers- en autorisatiegegevens kan zowel handmatig als automatisch geschieden.

Monitoring & audit
Eén van de grote voordelen van I AM is de mogelijkheid om continu te monitoren en dus te auditen. Met behulp van monitoring wordt het mogelijk om elk gewenst moment zicht te krijgen op de effectiviteit van het gebruikers(rechten)beleid ofwel *real-time audit*.

Met behulp van bovenstaande componenten kan I AM inspelen op de toegenomen noodzaak om het complexe landschap van gebruikers, autorisatie en informatieobjecten te managen dan wel te beheersen met als doel als organisatie '*in control*' te geraken en *operational excellence* te bereiken. Dit wordt gerealiseerd door enerzijds het reduceren van (operationele) risico's en dus het verhogen van informatiebeveiliging, en door anderzijds het realiseren van kostenbesparingen (verhogen productiviteit en lagere autorisatiebeheerkosten) en het verbeteren van gebruikersgemak.

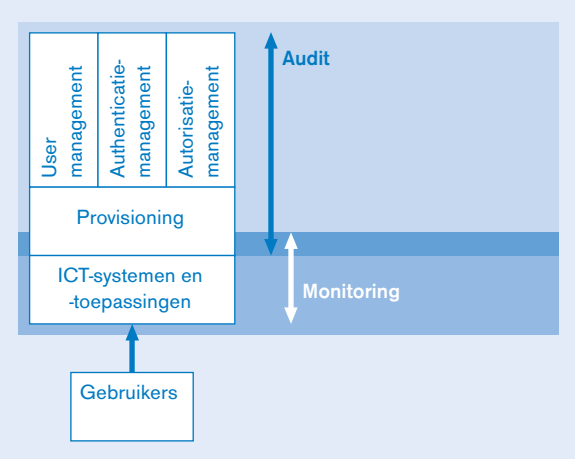
Mogelijkheden van I AM

De ervaring leert dat er meerdere redenen zijn waarom organisaties overwegen I AM in te voeren[1]. Daarbij is elke organisatie uniek en bestaat er niet zoiets als een 'one-size-fits-all' business case. Tabel 1 geeft een overzicht van de redenen (*drivers*) waarom organisaties de bijbehorende waardetoevoegende functionaliteiten van I AM overwegen.

Om te beginnen is er natuurlijk veel te doen rondom het onderwerp *compliance*. Dit wordt door veel organisaties als belangrijke reden genoemd om te beginnen met I AM ([Koor04]). De waarde van I AM zit dan in het bijzonder in het feit dat veelal handmatige processen om compliance aan te tonen (deels) worden geautomatiseerd. Bijvoorbeeld het vergelijken van daadwerkelijke toegang tot systemen ten opzichte van het gestelde beleid. Door deze geautomatiseerde afdwinging en rapportagemogelijkheden is het management ook echt in staat verantwoording af te leggen over de rechten van zijn gebruikers.

Vervolgens zien wij *risk management* als een belangrijke reden om I AM toe te passen. Nu is dit een thema dat zeker niet nieuw is voor organisaties en waar men al langere tijd toenemend systematisch mee bezig is. In dat kader implementeren organisaties wel meer maatregelen die bijdragen aan het verkrijgen van betere beheersing over hun informatievoorziening. Echter, juist

1) KPMG heeft hiernaar in 2004 onderzoek gedaan en de resultaten hiervan zijn in een eerdere editie van Compact gepubliceerd ([Koor04]).



Figuur 1. Samenhang I AM-componenten.

de huidige stand van zaken rondom diverse I AM-oplossingen en technologieën biedt hier nieuwe mogelijkheden, bijvoorbeeld ten aanzien van het real-time afdwingen van functiescheiding.

Procesverbetering (*process improvement*) gaat in op hoe I AM organisatorische veranderingen, zoals reorganisaties of verbetering van administratieve processen, kan faciliteren. Door toepassing van I AM kunnen bijvoorbeeld gemakkelijk en betrouwbaar gebruikers aan een nieuwe business unit worden toegewezen met bijbehorende nieuwe rollen en permissies. Ook het proces van toekennen van autorisaties kan door middel van geautomatiseerde workflows worden gestandaardiseerd en daardoor sneller worden uitgevoerd.

Ten slotte is er een duidelijke driver te onderkennen onder de noemer *technology improvement* ofwel algemene vernieuwing of modernisering van infrastructuren en applicatielandschappen. Na een periode van reorganisaties en kostenreducties is er een trend waarneembaar dat organisaties weer investeren in vernieuwing van IT-voorzieningen. Informatiebeveiliging in het algemeen is veelal een integraal onderdeel van een dergelijke vernieuwing en zeker aspecten rondom *identity* en *access* komen dan al snel naar voren bij het maken van investeringsvoorstellen en daaruit voortvloeiende architectuurkeuzen.

I AM in optima forma

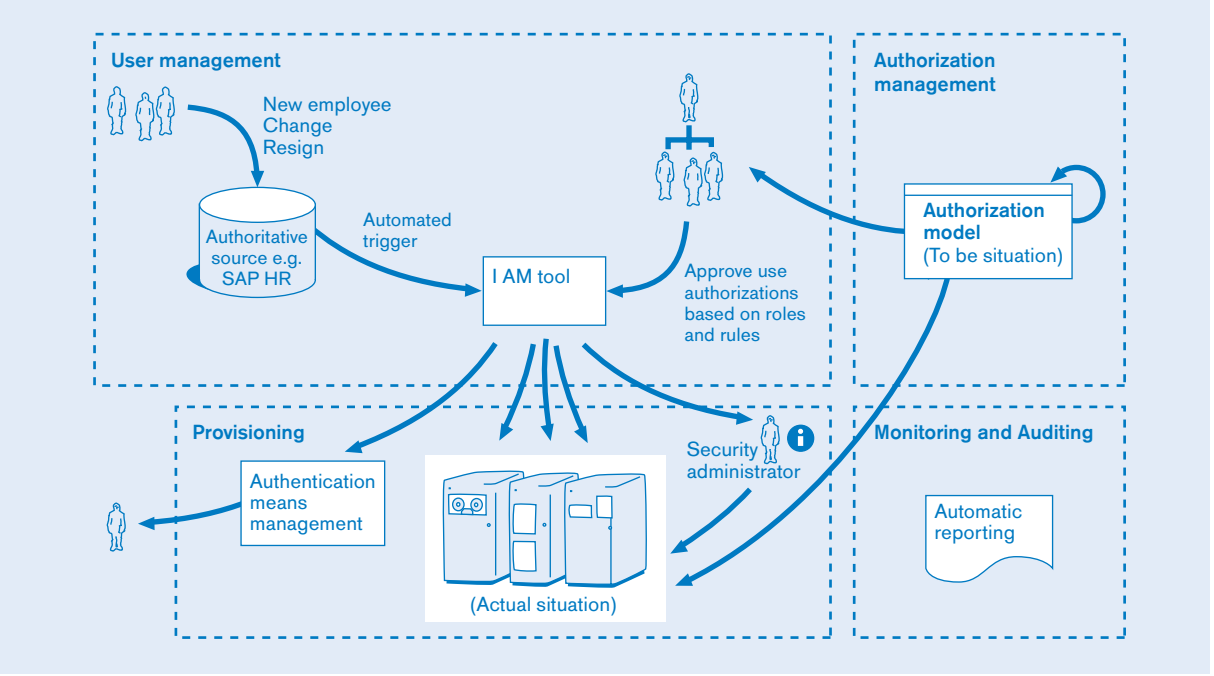
Figuur 2 geeft de 'optima forma' van I AM weer in termen van de eerder beschreven componenten. I AM start met wijzigingen in de bronregistratie van gebruikers (*authoritative source*). In dit voorbeeld is de bronregistratie van medewerkers de HR-administratie. In deze HR-administratie staan als het ware de stamgegevens van een medewerker. Tevens worden alle van belang zijnde gebeurtenissen, zoals indiensttreding (new employee), functiewijziging (change) en uitdiensttreding (resign), in deze bron geadministreerd.

Niet alleen compliance is reden om I AM in te voeren

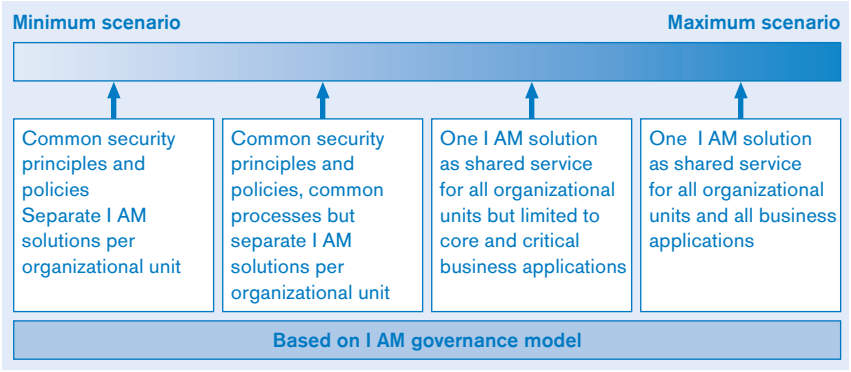
Deze gebeurtenissen zijn voor I AM van wezenlijk belang, aangezien zij initiërend werken voor het gehele user management. Zo 'triggeren' zij acties van leidinggevenden voor het uitgeven/intrekken van gebruikersaccounts en bijbehorende autorisaties. Het daadwerkelijk uitgeven/intrekken van de autorisaties wordt uitgevoerd door technisch en applicatiebeheer. Een geautomatiseerd hulpmiddel (I AM-tool) initieert deze acties en faciliteert het uitvoeren ervan, gebruikmakend van workflow. De leidinggevende krijgt op basis van een 'trigger' het signaal dat autorisaties goedgekeurd dienen te worden voor de betreffende medewerker op basis van een voorgedefinieerd autorisatiemodel (dat normaliter is gebaseerd op het gebruik van rollen en regels). Na akkoord zal de gebruiker voorzien worden van het juiste authenticatiemiddel en worden de noodzakelijke gebruikersaccounts en -autorisaties op een al of niet geautomatiseerde wijze gecreëerd en/of gemuteerd (*provisioning*) binnen de ICT-resources.

Driver	Pressures	I AM Value Proposition
Regulatory Compliance	Sarbanes Oxley GLBA Anti-Money Laundering Privacy Basel II Local corporate governance regulations	Improved Auditing and Logging Improved Monitoring Flexibility to Adapt to New Regulations Improved Reporting
Risk Management	Diverse Security Postures Increased Likelihood of Fraud Increased Security Risk	Reduce/Prevent Fraud Increased segregation of duties Better Enforcement of Policy Alignment of Financial System Access Controls
Process Improvement	Merger and Acquisition Activities Departmental Consolidation Diverse Business Mixes Off-shoring/Outsourcing Business Process Improvement Administrative Process Improvement	Consistent Security Quicker Rebranding of Services Quicker Integration of New Users Reduced Lost Productivity Reduced Costs Improved Workflow
Technology Improvement	Infrastructure Upgrades Applications Architecture Upgrades	Consistent Security Reduced Costs Reduced Licensing Fees Quicker time to Market with New Applications

Tabel 1. Drivers van I AM.



Figuur 2. I AM in 'optima forma'.



Figuur 3. Scenario's voor het ambitieniveau, gebaseerd op het I AM-governancemodel.

Ten slotte wordt er in de 'optima forma'-situatie voortdurend gecontroleerd of de gebruikersaccounts en -autorisaties zoals doorgevoerd binnen de ICT-resources (*actual situation*) nog steeds in overeenstemming zijn met de gewenste situatie (*to be situation*). Bij eventuele afwijkingen zal een zogenaamd incident-managementproces worden opgestart met als doel het evenwicht tussen *actual* en *to be* wederom te bereiken.

I AM in optima forma! I AM gericht op het bereiken van enerzijds maximale efficiency en anderzijds maximale control! De wens van iedere CIO, CFO, compliance officer en manager!

Impact van globalisering op het I AM-concept

Conceptueel staat het geschetste model als een huis. Echter, hoe valt dit te implementeren binnen een wereldwijd opererende organisatie, waarbij verscheidenheid een gegeven is? Verscheidenheid in tijdzones, geografische locaties, gebruikers (intern en extern), wetgeving, IT-middelen (platformen en applicaties) en IT-beheerconcepten.

De belangrijkste vraag die dan ook door een organisatie dient te worden beantwoord, is: *'Wat is het ambitieniveau dat de organisatie wenst en kan bereiken, rekening houdend met de (wereldwijde) IT-strategie van de organisatie?'*

Figuur 3 geeft het spectrum van het ambitieniveau weer in termen van mogelijke scenario's (van minimaal tot maximaal). Deze scenario's kunnen desgewenst tevens gezien worden als een groeimodel waarbij opschuiving van minimaal naar maximaal uiteraard voor de hand ligt (ook vanuit budgetteringsperspectief). Het is belangrijk op te merken dat het ambitieniveau en de haalbaarheid ervan in sterke mate worden bepaald door het I AM-governancemodel van een organisatie, dat antwoord geeft op vragen als wie het autorisatiemodel bepaalt en beheert (dus inclusief een wijzigingsprocedure).

We onderkennen de volgende vier scenario's:
1. *Gemeenschappelijk beleid en richtlijnen ten aanzien van I AM.* Hierbij wordt de implementatie van I AM-processen en -systemen overgelaten aan de verschillende organisatie-eenheden. Het resultaat is lokaal verschillende manieren van organisatie en ondersteuning van technologie, maar wel op basis van een gemeenschappelijk raamwerk.
2. *Gemeenschappelijk beleid, richtlijnen en I AM-processen.* Hoewel dit scenario al behoorlijk centralistisch van opzet is, worden er nog steeds afzonderlijke I AM-

systemen per organisatie-eenheid opgezet en beheerd. Qua gemeenschappelijkheid gaat dit scenario al een stap verder dan het eerste door ook dezelfde processen af te spreken (dus niet alleen strategisch maar ook op tactisch en operationeel niveau).
3. *Gemeenschappelijke I AM-oplossing bestaande uit beleid, richtlijnen, processen en infrastructuur*. In dit scenario wordt I AM-functionaliteit aangeboden als een shared service center[2], waarbij de dienstverlening zich richt op een beperkt aantal gemeenschappelijke, organisatiebrede systemen evenals bedrijfskritische toepassingen. Het inrichten van een shared service center ontslaat een organisatieonderdeel echter niet van de verantwoordelijkheid voor de juiste inrichting van de autorisaties. Een shared service center kan hierbij faciliterend optreden, maar het ontwikkelen en beheren van het autorisatiemodel is een verantwoordelijkheid van de business zelf. Het shared service center I AM is niet per definitie een zelfstandige organisatie-eenheid en zal vaak deel uitmaken van een overkoepelend shared service center.
4. *Organisatiebrede gemeenschappelijke I AM-oplossing*. Dit scenario is vergelijkbaar met de onder 3 genoemde vorm, met dien verstande dat het I AM-shared service center zich richt op alle organisatieonderdelen, platformen en toepassingen binnen een organisatie.

Om nu vervolgens de strategie ten aanzien van I AM en de invulling ervan te kunnen bepalen, biedt tabel 2 een vergelijking op basis van de volgende elementen of criteria:
- *Operational excellence*: kwaliteit en professionaliteit van de I AM-processen. Naast kwaliteit (en betrouwbaarheid als onderdeel daarvan) is snelheid van juiste toewijzing van autorisaties een factor in het verhogen van arbeidsproductiviteit van gebruikers die immers sneller toegang zullen verkrijgen tot de juiste informatie.
- *Mate van 'control'*: in hoeverre kunnen het geldende beleid en richtlijnen worden afgedwongen. Dit element wordt sterk bepaald door het governancemodel van de organisatie ofwel hoe autonoom zijn landenorganisaties in relatie tot het hoofdkantoor. En meer in IT-termen gesteld: bestaat er een referentiearchitectuur?, is er een preferred-supplierbeleid?, etc.
- *Benodigde investeringen*: hoe verhouden de benodigde investeringen zich tot beschikbare budgetten en ook in relatie tot budgetten voor informatiebeveiliging en upgrade van IT-infrastructuur in het algemeen.
- *Te realiseren besparingen ('benefits')*: hoe gedetailleerd zijn te verwachten besparingen doorgerekend en hoe kunnen ze worden gemeten. Denk hierbij aan het verminderen van werkzaamheden van (lokale) applicatiebeheerders maar ook aan vermindering van kosten gerelateerd aan de helpdesk.

In de praktijk komen de eerdergenoemde scenario's allemaal voor. Het scenario wordt voornamelijk bepaald door (IT-)strategie, governance en cultuur binnen de organisatie. Immers, in een gedecentraliseerde organisatie met grote lokale bevoegdheden en onafhankelijkheden, is scenario 1 en/of 2 maximaal haalbaar, terwijl een sterk gecentraliseerde organisatie met strikte governance het mogelijk maakt scenario 3 of zelfs 4 te realiseren.

De conclusie uit tabel 2 is dat indien een organisatie het optimale rendement wil behalen ten aanzien van I AM op de criteria *operational excellence* en mate van control (*compliance*) voor de gehele organisatie (zoals beschreven in de paragraaf 'Mogelijkheden van I AM') scenario 1 zeker niet nagestreefd dient te worden. Scenario 2 is de situatie die we in de praktijk nog het meeste aantreffen. Er wordt dan al zeer nadrukkelijk gezocht naar synergievoordelen door gemeenschappelijkheid, maar tegelijkertijd wil men veelal nog lokale technische oplossingen instandhouden. Dit gebeurt niet in de laatste plaats door hoge werkdruk van IT-organisaties en schaarse kennis op het vlak van informatiebeveiliging, IT-infrastructuren en I AM.

2) Een shared service center (SSC) is volgens de definitie van Strikwerda 'een resultaatverantwoordelijk samenwerkingsverband dat tot taak heeft het leveren van diensten op een specifieke specialisatie aan de afzonderlijke moederorganisaties op basis van een overeenkomst tegen een verrekenprijs'.

Opkomst van I AM-shared service centers binnen internationaal opererende organisaties

Als we bovenstaande scenario's toepassen op een grote internationaal opererende organisatie, zien we scenario 3, het realiseren van een zogenaamd I AM-shared service center (I AM-SSC) als het maximaal haalbare. Vergelijkbaar met reeds meer in zwang geraakte SSC's voor HR en financiële processen kunnen de onderstaande voordelen worden gerealiseerd door gelijksoortige functies, systemen, processen en resources te bundelen en deze vervolgens optimaal te ontwikkelen en exploiteren.

De volgende drie doelstellingen van een dergelijk I AM-SSC kunnen worden onderkend:
- schaalvoordelen realiseren;
- kwaliteit en professionaliteit van de dienstverlening verbeteren (*operational excellence*);
- regie krijgen en behouden ('*in control*').

Tabel 2. Vergelijking scenario's op basis van vier criteria.

Scenario	Operational excellence	Mate van control	Benodigde investeringen	Te realiseren besparingen
1	--	-/0 (afhankelijk van mate van governance)	Beperkt	Laag
2	+	0/+	Zeer hoog	Beperkt
3	++	+(+)	Hoog	Hoog
4	++	++	Zeer hoog	Hoog

1. Gemeenschappelijk beleid en richtlijnen ten aanzien van I AM.
2. Gemeenschappelijk beleid, richtlijnen en I AM-processen.
3. Gemeenschappelijke I AM-oplossing bestaande uit beleid, richtlijnen, processen en infrastructuur.
4. Organisatiebrede gemeenschappelijke I AM-oplossing.

De volgende bijbehorende diensten van een I AM-SSC kunnen worden onderkend (in relatie tot de I AM-processen zoals reeds beschreven in de paragraaf 'Wat is I AM?'):

- het inrichten van de workflow benodigd voor de geautomatiseerde interactie tussen autorisatieaanvragers en I AM-SSC;
- het optreden als I AM-loket/supportfunctie voor zowel de autorisatieaanvragers als de eindgebruikers (user management);
- het technisch beheren van de autorisatiemodellen op basis van rollen en regels die zijn vastgesteld door de organisatieonderdelen (deel van het autorisatiemanagement);
- het realiseren van benodigde geautomatiseerde koppelingen naar de verschillende systemen (provisioning);
- het verstrekken van de benodigde informatie aan de organisatieonderdelen, benodigd voor het aantonen van compliance (monitoring & audit).

I AM-SSC: wat is de rol van de organisatieonderdelen?

Zoals in de vorige paragraaf beschreven kan door het I AM-SSC een groot aantal, met name technische en operationele I AM-processen worden uitgevoerd, op een zo efficiënt mogelijke wijze. Wat echter zeker niet onderbelicht dient te worden is rol van de verschillende organisatieonderdelen. Wil een organisatieonderdeel gebruik kunnen maken van de diensten van het I AM-SSC, dan dient het I AM-SSC te beschikken over het autorisatiemodel van het organisatieonderdeel. Immers, in het 'optima forma' I AM-model zal een manager gebruikmaken van een geautomatiseerde workflow voor het aanvragen en wijzigen van autorisaties, waarin hij kan kiezen uit een voorgedefinieerde set van rollen, beschreven in het autorisatiemodel.

In de praktijk wordt de nadruk gelegd op óf compliance óf operational excellence

Het ontwerpen van dit autorisatiemodel, waarin daadwerkelijk bepaald en beschreven is wat iemand nu eigenlijk mag, is iets wat te allen tijde door de bedrijfsonderdelen zelf dient te geschieden. Het I AM-SSC kan hiervoor nooit verantwoordelijk worden gesteld, aangezien het I AM-SSC niet beschikt over de benodigde bedrijfs- en proceskennis om te kunnen bepalen hoe deze autorisatiemodellen dienen te worden opgesteld voor de verschillende bedrijfsonderdelen.

De maximale rol die het I AM-SSC kan spelen, is het totstandkomings- en onderhoudsproces van deze autorisatiemodellen[3] te faciliteren om te komen tot de benodigde autorisatiemodellen.

3) In de Compact-special over informatiebeveiliging, welke medio 2007 verschijnt, zal het opstellen van een autorisatiemodel op basis van rollen diepgaand worden behandeld.

Conclusie

Het verstrekken van autorisaties en de controle hierop worden steeds complexer voor internationale organisaties, vanwege onder andere steeds mobieler wordende medewerkers (Martini-concept), stringente wet- en regelgeving en de stroom aan organisatiewijzigingen. Organisaties kunnen voordelen realiseren door hierop te anticiperen in de vorm van het ontwikkelen en implementeren van een I AM-strategie.

Bij het definiëren van de I AM-strategie staan het bepalen van het ambitieniveau en de (on)mogelijkheden vanuit internationaal perspectief ten aanzien van I AM centraal. Allereerst dient de organisatie te bepalen wat de belangrijkste drijfveren voor I AM zijn, te weten compliance of operational excellence. Uiteraard kan een organisatie beide nastreven, maar uit de praktijk blijkt dat toch de nadruk wordt gelegd op één van de twee aspecten. Dit onderscheid kan ook naar voren komen in een groeimodel, waarbij een organisatie eerst een aantal quick wins behaalt door zaken als wachtwoordsynchronisatie en elektronische autorisatieaanvragen (operational excellence) te realiseren en vervolgens aan de slag te gaan met het verbeteren van het autorisatiemodel (compliance).

Na het bepalen van de focus ten aanzien van I AM dient de organisatie het meest optimale scenario te selecteren. Het spectrum loopt hierbij van alleen een gemeenschappelijk I AM-beleid tot een gecentraliseerde of geconcentreerde (gezamenlijk ten behoeve van organisatorische eenheden) I AM-oplossing waarbij gebruik wordt gemaakt van een I AM-shared service center voor alle organisatieonderdelen, platformen en applicaties.

Onze conclusie is dat voor een internationale organisatie het optimale scenario een gemeenschappelijke I AM-oplossing is, gebruikmakend van een I AM-shared service center voor een beperkt aantal gemeenschappelijke, organisatiebrede systemen evenals voor de bedrijfskritische toepassingen.

Literatuur

[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.