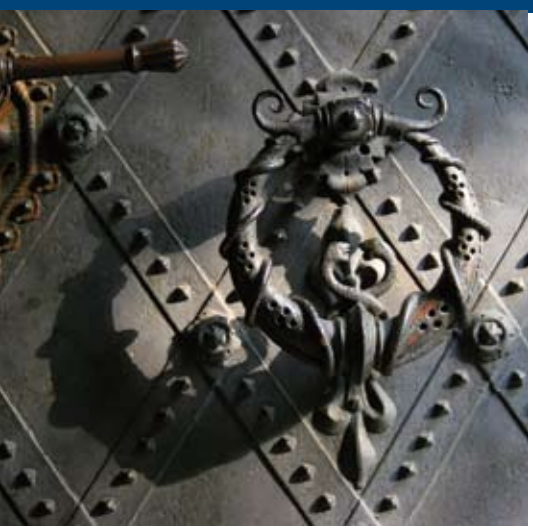


KPMG's Identity and Access Management Survey 2008

Ing. J.A.M. Hermans RE
is director bij KPMG IT Advisory te Amstelveen. Binnen KPMG is hij verantwoordelijk voor de Identity & Access Management-dienstverlening 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-methodologie.

hermans.john@kpmg.nl

P.E. van der Hulst
is adviseur bij KPMG IT Advisory te Amstelveen. In zijn dagelijkse werkzaamheden begeleidt hij organisaties als projectmanager bij het implementeren van Identity & Access Management-concepten.

vanderhulst.emanuel@kpmg.nl

P. Ceelen MSc
is junior adviseur bij KPMG IT Advisory te Amstelveen en richt zich voornamelijk op Identity en Access Management en technische uitdagingen die bij deze projecten spelen.

ceelen.pieter@kpmg.nl

G. van Gestel MSc
was werkzaam bij KPMG IT Advisory te Amstelveen, na zijn afstudeerstage bij ICT Security and Control te hebben afgerond op het gebied van Identity and Access Management. Sindsdien heeft hij allerlei opdrachten uitgevoerd op het gebied van audit, assurance en Identity and Access Management.

Ing. John Hermans RE, Emanuël van der Hulst, Pieter Ceelen MSc en Geo van Gestel MSc

In februari 2008 heeft KPMG IT Advisory een onderzoek gehouden onder Europese organisaties naar Identity and Access Management ([Hermo8]). De vragen uit het onderzoek richtten zich op IAM-initiatieven. Wat zijn de toegekende budgetten voor projecten? Hoeveel projecten zijn er in de afgelopen tijd gestart? Waarom beginnen organisaties met IAM? Wat zijn de verwachte voordelen van de IAM-projecten en zijn organisaties wel tevreden over de IAM-projecten? Als laatste wordt er ook gekeken naar de volwassenheid van IAM-omgevingen bij de deelnemende organisaties. Dit artikel geeft een beknopte weergave van de bevindingen van het onderzoek. Een volledig onderzoeksrapport is verkrijgbaar via kpmg.nl.

Informatie, een waardevolle bezitting

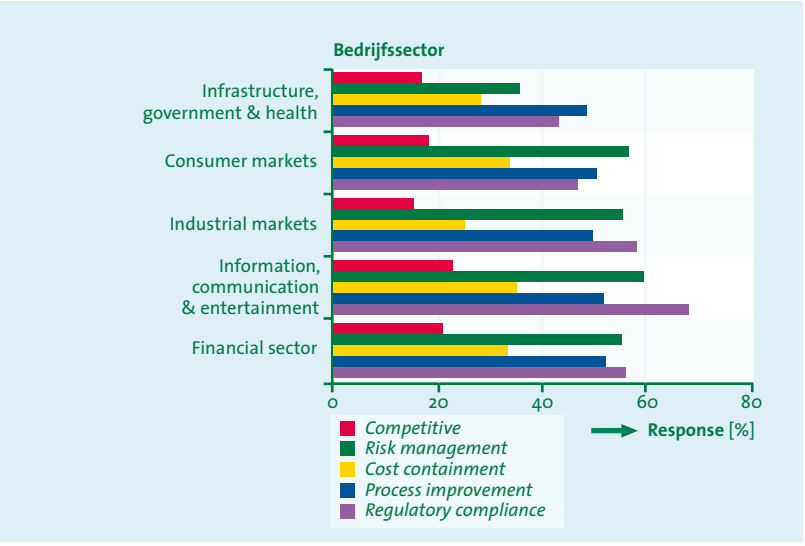
Informatie is één van de meest waardevolle bezittingen van een organisatie. Beheer van de toegang tot deze informatie is tegenwoordig een belangrijk onderdeel van de bedrijfsvoering. Externe en interne belanghebbenden stellen steeds hogere eisen aan de borging van de beveiliging van deze informatie binnen organisaties.

Dat bedrijven de druk van externe en interne belanghebbenden onderkennen, blijkt uit het feit dat alle deelnemers de afgelopen drie jaar één of meer Identity and Access Management (IAM)-projecten hebben uitgevoerd. Tweederde van de deelnemende bedrijven heeft een budget specifiek voor IAM. De IAM-specifieke budgetten variëren van € 10 tot € 600 per werknemer per jaar. Het gemiddelde budget ligt rond de € 200 per jaar. Binnen de financiële sector liggen deze budgetten ongeveer twintig procent hoger ten opzichte van de andere sectoren ([Hermo8]).[1]

Ondersteuning interne processen

De soms forse investeringen die worden gedaan op het gebied van IAM worden niet alleen gedaan vanwege externe factoren, zoals wet- en regelgeving. Deelnemers geven aan dat

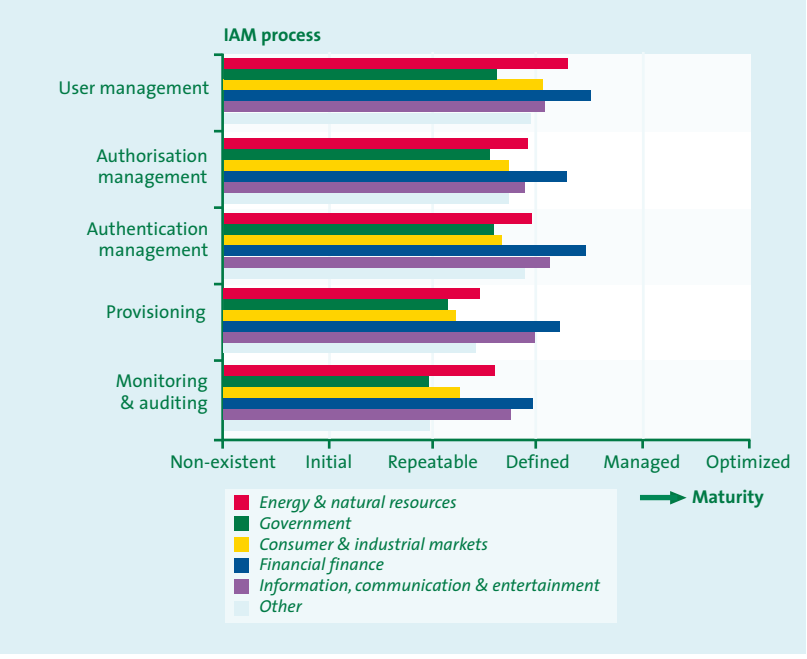
1) ICE: Information, communication and entertainment; FS: Financial sector; IGH: Infrastructure, government and healthcare; IM: Industrial markets; CM: Consumer markets.



Figuur 1. **Drijfveren voor IAM-initiatieven per bedrijfssector.**

risicobeheer en verhoging van de 'business value' ook belangrijke drijfveren zijn om IAM-initiatieven te starten.

De motieven kostenbeheersing en competitieve voordelen spelen een minder grote rol bij het opstarten van IAM-initiatieven. Vooral binnen de financiële sector en de sector informatie, communicatie en entertainment wordt de naleving van wet- en regelgeving en risicobeheer gezien als de belangrijkste drijfveer voor IAM-projecten. Voor de sector infrastructuur, overheid en gezondheidszorg zijn deze drijfveren het minst belangrijk, organisaties uit deze sector verwachten verhoging van de 'business value' door middel van procesverbeteringen. De onderzoeksresultaten lieten binnen de Europese regio's geen significante verschillen zien met betrekking tot deze motieven.



Figuur 2. **Volwassenheidsniveaus per marktsector.**

Aangezien de eisen van wet- en regelgeving vooral geënt zijn op interne bedrijfsvoering, is het verklaarbaar dat IAM-initiatieven gericht zijn op interne processen en informatie. De initiatieven zijn veelal gericht op toegang tot informatie van eigen werknemers en inhuurkrachten en in mindere mate op de toegangsrechten van derde partijen zoals leveranciers.

Groeiend in alle opzichten

Uit het onderzoek blijkt dat IAM-processen binnen veel organisaties gemiddeld volwassen zijn. Processen worden gestandaardiseerd en gedocumenteerd, waardoor ook hun uitvoering kan worden gecontroleerd en gereproduceerd. Het gemiddelde volwassenheidsniveau over de regio's en processen heen ligt op de niveaus 'managed' en 'defined'[2] (zie figuur 2). Onderling is er tussen de regio's geen groot verschil, alleen heeft de regio Noord-Europa een hoger gemiddeld volwassenheidsniveau.

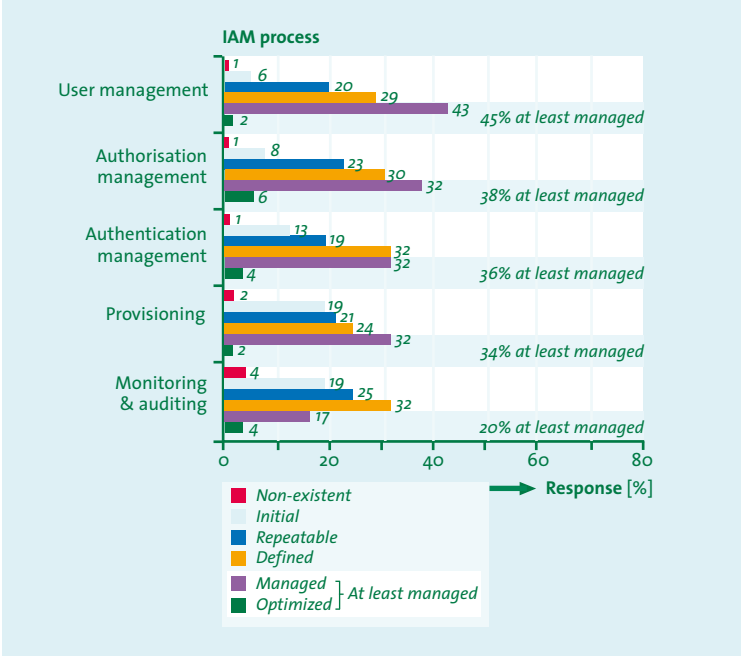
Wanneer er naar de volwassenheid wordt gekeken tussen sectoren onderling (figuur 2), wordt duidelijk dat binnen de financiële sector alle IAM-processen op een hoger volwassenheidsniveau zitten. Een verklaring hiervoor kan zijn dat organisaties in de financiële sector onderhevig zijn aan striktere internecontroldiensten en externe wet- en regelgeving.

Bij het overgrote deel van de respondenten blijken de IAM-processen echter nog onder het niveau 'managed' (zie figuur 3) te zitten. Dit betekent dat organisaties hun processen wel gestandaardiseerd en gedocumenteerd hebben, maar dat er nog niet wordt gekeken naar de prestaties en kwaliteit van deze processen.

Tevredenheid niet naar verwachting

Ondanks het feit dat de IAM-initiatieven zich niet meer in de opstartfase bevinden wat betreft volwassenheidsniveau, worden niet alle verwachtingen gerealiseerd door de IAM-initiatieven. Met betrekking tot de tevredenheid over de resultaten van de IAM-initiatieven tonen de resultaten uit het onderzoek aan dat de behaalde resultaten niet volledig voldoen aan de verwachtingen (zie figuur 4). 11 procent van de deelnemers geeft aan zeer tevreden te zijn, terwijl 39 procent enigszins tevreden

2) Het volwassenheidsmodel ([Gesto7]) is gebaseerd op Cobit en kent de volgende niveaus: non existent, initial, repeatable, defined, managed en optimized.



Figuur 3. **Volwassenheidsniveaus per IAM-proces.**

is over resultaten van de IAM-projecten. De antwoorden van de overige deelnemers variëren van 'zeer ontevreden' (4 procent) tot 'neutraal' (27 procent).

Met de stelling 'Inzicht in de voordelen van IAM ontbreekt in mijn organisatie' is tweederde van de respondenten het eens. Dat de meerderheid van de respondenten beaamt dat ze te weinig inzicht hebben in de voordelen van IAM, verklaart wellicht de relatief lage graad van tevredenheid over IAM-initiatieven (zie figuur 5). Uit de antwoorden van de respondenten blijkt dat de helft van de projecten faalt doordat de bedrijfsvoering nog niet klaar is voor de in het IAM-initiatief voorgestelde oplossing.

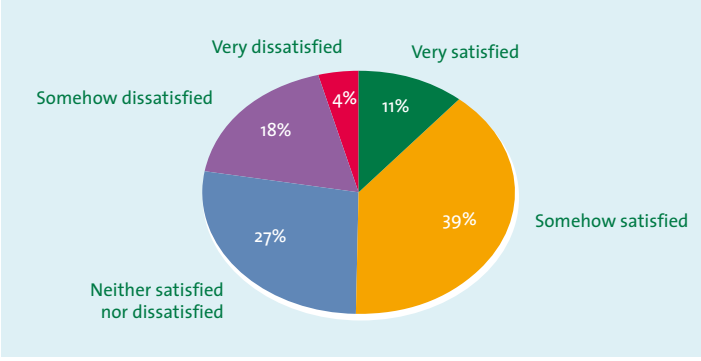
Het falen van de IAM-projecten kan worden verklaard doordat de initiatieven te veel gericht zijn op het implementeren van IT-oplossingen. Verantwoordelijkheid voor de strategie voor IAM ligt bij veel organisaties bij de IT-medewerkers (bijvoorbeeld de security officer of het hoofd van de afdeling IT). Door de meer technische insteek komt het voor dat er onvoldoende aandacht uitgaat naar de integratie van de technische oplossing met de bestaande bedrijfsprocessen.

Concluderend: IAM is here to stay!

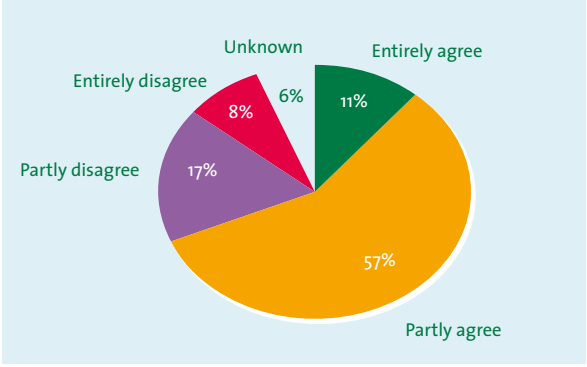
In de afgelopen jaren is er veel geschreven en gezegd over IAM. Velen dachten dat het een hype was, echter mogen we op basis van dit onderzoek wel concluderen dat IAM een duurzame ontwikkeling is ('IAM is here to stay!'). Organisaties hebben toegevoegde waarde van IAM-initiatieven onderkend en geïnvesteerd in de onderliggende processen en technieken.

Naast toegevoegde waarde voor organisaties op het gebied van performanceverbetering (operational excellence) is IAM ook een goed antwoord op de wet- en regelgeving aangaande informatiebeveiliging. Deze wetten roepen om verantwoording en transparantie omtrent gebruik van vertrouwelijke informatie. Door het invoeren van gestructureerde IAM-processen worden dus ook externe belanghebbenden tegemoetgekomen.

Nu duidelijk is dat IAM toegevoegde waarde kan leveren aan een organisatie, dienen bedrijven alleen nog te werken aan de professionalisering van hun IAM-initiatieven, zo blijkt uit dit onderzoek. Aspecten als commitment van de juiste stakeholders in de organisatie en verwachtingsmanagement spelen hierbij een cruciale rol. Immers, het implementeren van IAM is niet alleen een technologisch project, maar met name een project dat de organisatie en processen raakt. Kortom: 'get the business involved'!



Figuur 4. **Tevredenheid over IAM-initiatieven.**



Figuur 5. **Gebrek aan inzicht van IAM-initiatieven.**

Respondents	% (n=235)	
Geographical region		
North *(UK, Scandinavia, Baltics)*	17	
East *(Bulgaria, Poland, Hungary, Czech Republic, Romania, Slovakia)*	11	
South *(Italy, Spain, Portugal)*	15	
West *(Benelux, Germany, Switzerland, Austria)*	57	
	100	
Size of organisation (#users)		
<5,000	59	
5,000 – 10,000	14	
>10,000	27	
	100	
Organisation sector		
Consumer markets	13	
Financial services	41	
Industrial markets	20	
Information, communication & entertainment	11	
Infrastructure, government & health	15	
	100	

Tabel 1. **Geografische en industriële verdeling van enquête-participanten.**

Onderzoeksopzet

De resultaten uit het onderzoek zijn afkomstig van 235 respondenten, uit 21 Europese landen. De opbouw van de groep respondenten varieert van CEO's en CIO's tot aan security officers en hoofden van de interne auditafdeling. De respondenten zijn werkzaam bij organisaties van verschillende formaten en uit vijf verschillende sectoren (zie tabel 1).

De enquête van het onderzoek werd elektronisch beschikbaar gesteld gedurende een periode van twee weken. De enquête bestond uit gesloten vragen over de tevredenheid, status en volwassenheid van IAM-initiatieven. De vragen waren verdeeld over vier onderdelen: algemene data, organisatiedata, data over beveiliging en IAM-volwassenheid. De resultaten zijn na sluiting van de enquête verwerkt in een officieel onderzoeksrapport, dat op 23 april 2008 werd gepubliceerd tijdens de Kuppinger Cole-conferentie in München.

Identity and Access Management: de basis

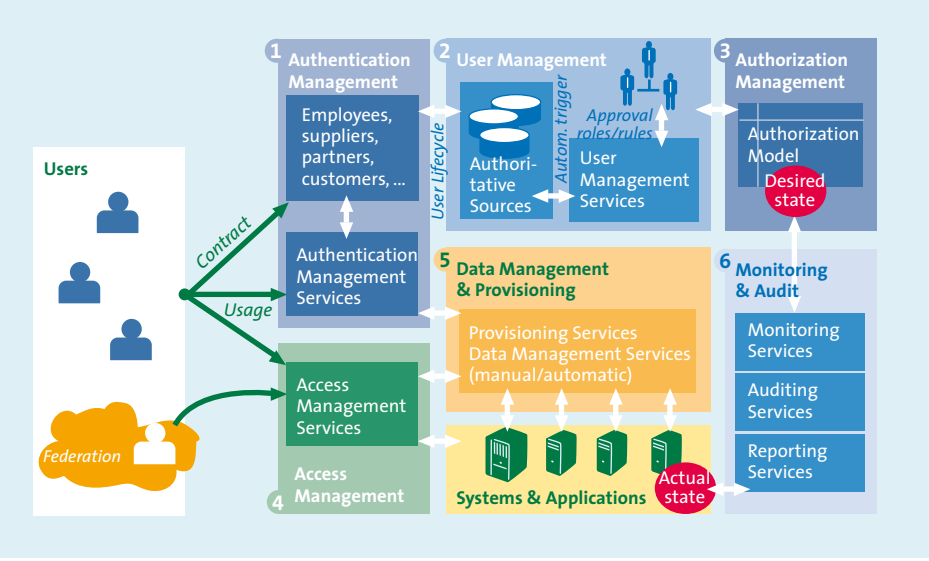
Aan de basis van het onderzoek ligt het Identity and Access Management (IAM)-raamwerk van KPMG. Binnen het onderzoek is IAM als volgt gedefinieerd:

'De verzameling van processen, beleid en systemen die efficiënt en effectief beheren, wie toegang tot welke bronnen binnen een organisatie heeft.'

De verzameling van processen, beleid en systemen is onder te verdelen in vijf deelgebieden, namelijk:

- *User management:* activiteiten gericht op het beheer van de gehele levenscyclus van gebruikers.
- *Authentication management:* activiteiten gericht op het beheren van de gegevens die nodig zijn voor het valideren van de identiteit van een persoon (authenticatiegegevens) en de mate van validatie die in ICT-systemen en -toepassingen moet worden vastgelegd (zoals vereiste authenticatiesterktes en beleidsregels).

Figuur 6. **IAM-raamwerk ([Hermo8]).**



Figuur 7. **IAM-referentiemodel.**

- *Authorisation management:* activiteiten gericht op het beheer van rechten op de doelsystemen (autorisaties) van gebruikers (medewerkers).
- *Provisioning:* betreft het handmatig en/of geautomatiseerd propageren van gebruikers- en autorisatiegegevens naar ICT-systemen en toepassingen.
- *Monitoring & audit:* betreft logging, auditing en rapportage.

Literatuur

[Gesto7] Geo van Gestel, *Creating an Identity and Access Management Maturity model*, december 2007.

[Hermo8] John Hermans, *KPMG's 2008 European Identity and Access Management Survey*, maart 2008.