Identity & Access Management: operational excellence of 'in control'?

Ing. J.A.M. Hermans RE en drs. J. ter Hart

Identity & Access Management staat binnen de meeste organisaties volop in de belangstelling, vanwege enerzijds het streven naar operational excellence (kostenbesparing en verbeteren van gebruikersvriendelijkheid) en anderzijds het moeten voldoen aan interne en externe wet- en regelgeving, die onder meer een goed ingericht Identity & Access Management vereisen. Dit artikel gaat in op hoe een organisatie een dergelijk Identity & Access Management-programma kan starten, met aandacht voor de business case (het waarom), de blauwdruk (het wat) en de roadmap (het hoe). In de beschrijving van business case, blauwdruk en roadmap zullen tevens enkele voorbeelden uit de praktijk worden gegeven.

Inleiding

Identity & Access Management, een paraplubegrip voor een veelvoud van termen, is één van de programma's die op dit moment binnen een organisatie sterk in de belangstelling staan. Voornaamste drijfveren zijn het streven naar operational excellence (het beter doen tegen lagere kosten) alsook het moeten voldoen aan eisen zoals gesteld door wet- en regelgeving (waaronder Sarbanes-Oxley, Basel II, Wet bescherming persoonsgegevens).

Door de veelheid aan aspecten waarmee binnen een Identity & Access Management-programma rekening dient te worden gehouden, is een Identity & Access Management-programma geen sinecure. Wat is het? Waarom op dit moment? Waar te beginnen? Hoe aan te pakken? Hoe te zorgen dat de projecten in het programma het gewenste eindresultaat opleveren? Dit is slechts een korte opsomming van vragen die binnen organisaties leven op het moment dat een Identity & Access Management-programma wordt geïnitieerd.

Teneinde goed gefundeerd een Identity & Access Management-programma te initiëren, is het dan ook van belang om te starten met het identificeren en vaststellen van de uitgangspunten door het opstellen van de business case voor Identity & Access Management. Nadat deze case akkoord is bevonden door het hoogste management, kan daadwerkelijk gestart worden met de verdere uitwerking, en wel met het definiëren van het toekomstige concept (de blauwdruk) en het opstellen van de roadmap: de beschrijving van de benodigde stappen om het toekomstige concept te realiseren.

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. J. ter Hart
is consultant 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@kmpg.nl

In dit artikel zal verder worden ingegaan op de business case, blauwdruk en roadmap ten aanzien van Identity & Access Management, onderdelen van een door KPMG Information Risk Management ontwikkelde gefaseerde, overkoepelende programma-aanpak, 'Identity & Access Management (I AM) in control' (zie [Koor04]).

Identity & Access Management: een introductie

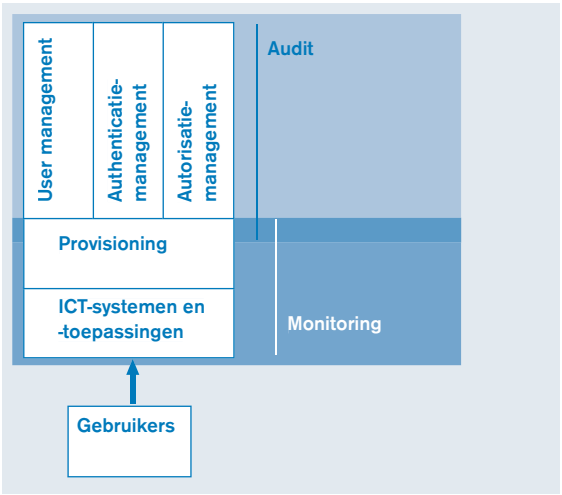
Een behoorlijk aantal organisaties in verschillende branches overweegt om een Identity & Access Management-programma (I AM) te starten of heeft de eerste stappen richting I AM gezet. Het is dan ook niet verwonderlijk dat er in de vakliteratuur en tijdens congressen en seminars veel aandacht aan I AM wordt besteed. Maar wat wordt nu eigenlijk met I AM bedoeld? In dit artikel gaan we uit van de volgende omschrijving (gebaseerd op [Koor04]):

Identity & Access Management:
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.

Binnen I AM wordt onderscheid gemaakt tussen de volgende componenten:
- *User management*: activiteiten gericht op het beheer van de gehele cyclus van een persoon (indiensttreding, functiewijziging, ontslag);
- *Authenticatiemanagement*: activiteiten gericht op het beheer van authenticatiemiddelen (password, tokens, etc.);
- *Autorisatiemanagement*: activiteiten gericht op het beheer van autorisaties van gebruikers;

Figuur 2. Noodzaak voor I AM

Verleden	Heden
• Relatief beperkt aantal resources met toegekende autorisaties • Alleen toegang tot systemen via eigen netwerk • Alleen autorisaties voor eigen medewerkers • Klein aantal autorisaties per medewerker/gebruiker • Relatief eenvoudige administratieve afhandeling • Beperkte invloed wet- en regelgeving	• Groot aantal verschillende resources, ieder met eigen authenticatie- en autorisatiemodules • Zowel medewerkers als partners, klanten en leveranciers krijgen toegang tot resources • Toenemend aantal communicatiekanalen door nieuwe vormen van dienstverlening • Meerdere autorisaties per gebruiker, bijvoorbeeld verschillende authenticatiemiddelen • Meerdere administratoren, vaak georganiseerd per platform en/of toepassing • Complexe en dure administratieve afhandeling door diversiteit aan processen • Invloed wet- en regelgeving toegenomen (Wbp, SOX, Basel II) • Noodzaak kostenbeheersing toegenomen



Figuur 1. Samenhang I AM-componenten.

- *Provisioning*: het (handmatig en/of geautomatiseerd) doorvoeren van gebruikers- en autorisatiegegevens naar (ICT-)objecten;
- *Monitoring & audit*: logging, (permanente) auditing en rapportage.

De samenhang tussen deze verschillende componenten is in figuur 1 weergegeven.

De toegevoegde waarde / noodzaak van I AM

Sinds het begin van IT wordt er al aandacht besteed aan logische toegangsbeveiliging. Waarom nu dan ineens die aandacht voor I AM? Een belangrijke reden is gelegen in het feit dat oude oplossingen niet meer voldoen in de dynamische omgeving van nu (zie figuur 2).

Op basis van figuur 2 kan worden gesteld dat er voor I AM eigenlijk twee categorieën drijfveren aanwezig zijn, te weten operational excellence en het streven naar 'in control'. In de praktijk worden deze twee categorieën meestal gecombineerd.

Operational excellence

Bij operational excellence spelen het realiseren van kostenbesparingen en het verbeteren van het gebruikersgemak een belangrijke rol.

Kostenbesparingen kunnen worden gerealiseerd door het stroomlijnen, harmoniseren en consolideren van de operationele I AM-processen. Daarnaast wordt de beheersbaarheid van de toegangsverlening verbeterd doordat door de inzet van één I AM-systeem de complexiteit ten aanzien van I AM wordt verminderd. Bij het opstellen van de business case voor I AM moet echter

gewaakt worden voor te positieve berekeningen met betrekking tot de Return on Investment (RoI). In de praktijk is het namelijk lastig om de huidige kosten gerelateerd aan Identity & Access Management in kaart te brengen. Deze worden als zodanig zelden herkend en erkend. Tevens zullen kostenbesparingen gerelateerd aan operational excellence niet automatisch leiden tot afvloeiing van personeel, maar vindt er ook een verschuiving plaats naar het tactisch autorisatiemanagement (bijvoorbeeld het beheer van rollen).

Het tweede aspect van operational excellence, de verbetering in het gebruikersgemak, wordt onder andere gerealiseerd doordat:
- het aantal te gebruiken gebruikersaccounts en wachtwoorden wordt gereduceerd (Reduced Sign On);
- de mogelijkheid wordt geboden om een password self-service in te richten waar gebruikers zelf hun wachtwoord kunnen resetten zodat daarmee de belasting van de helpdesk afneemt;
- de doorlooptijd voor de verwerking van de aanvraag van een nieuwe autorisatie behoorlijk wordt verkort.

'In control'

Een belangrijk aspect bij het streven naar 'in control' is het reduceren van (operationele) risico's, evenals het verhogen van het niveau van informatiebeveiliging doordat de organisatie aantoonbaar 'in control' zal zijn ten aanzien van Identity & Access Management. Het feit dat met behulp van I AM de verantwoordelijkheden op een eenvoudige wijze bij de juiste personen kunnen worden belegd, draagt ook in belangrijke mate bij aan het 'in control' zijn van een organisatie. Het lijnmanagement is namelijk verantwoordelijk voor het tactisch management, terwijl de operationele uitvoering aan de ICT-afdeling is toebedeeld. De verantwoordelijkheidsverdeling is in tegenstelling tot de dagelijkse werkelijkheid in het merendeel van de organisaties. Onder tactisch management wordt verstaan: het koppelen van rollen aan gebruikers, het definiëren van nieuwe rollen en het wijzigen hiervan. Deze taken moeten worden uitgevoerd op basis van vastgesteld I AM-beleid. Het tactisch management vervult een soort van Change Advisory Board-rol. De beslissingen van het tactisch management worden geoperationaliseerd door het operationeel management (ICT-afdeling). Deze afdeling voert de wijzigingen in het rollenmodel daadwerkelijk door in het I AM-systeem.

Een ander aspect bij het 'in control' zijn is natuurlijk het voldoen aan de relevante wet- en regelgeving zoals de Wet bescherming persoonsgegevens (Wbp) en Sarbanes-Oxley (SOX). In het kader van SOX speelt I AM een zeer belangrijke rol. Een organisatie kan namelijk niet SOX-compliant zijn zonder een adequate logische toegangsbeveiliging. Meerdere best practices die ontwikkeld zijn in het kader van SOX-compliancy noemen de volgende controledoelstellingen:
- Toegangsrechten tot ICT-systemen en -resources dienen alleen toegekend te zijn in overeenstemming met de exacte behoeften zoals gedefinieerd door de functieomschrijving/rol in de organisatie.
- Organisaties dienen aan te tonen dat alleen geautoriseerde gebruikers toegang hebben tot 'gevoelige' informatie en systemen.
- Het is noodzakelijk om de gebruikelijke internecontrolemaatregelen, zoals functiescheiding, af te dwingen.
- Periodieke beoordeling van toegangsrechten en privileges is vereist.

SOX vereist niet zozeer een I AM-oplossing, maar het 'in control' zijn inzake I AM-processen. Door inzet van I AM-tooling kan de 'in control'-status op een effectieve en efficiënte wijze worden bereikt. Hierbij kan de vergelijking worden gemaakt met boekhouden. Een organisatie die dit handmatig uitvoert is zeer veel tijd kwijt aan het boekhouden en de controle op de gehele administratie. Geautomatiseerde ondersteuning maakt het efficiënter,

Een organisatie kan niet SOX-compliant zijn zonder een adequate logische toegangsbeveiliging

waarbij ook technische maatregelen kunnen worden geïmplementeerd ten behoeve van de betrouwbaarheid. Met behulp van I AM kunnen de genoemde controledoelstellingen worden gehaald. Een I AM-oplossing biedt een organisatie de mogelijkheid om alle identiteiten en bijbehorende autorisaties effectief te beheren. Doordat in één systeem de toegang tot alle kritieke en vertrouwelijke informatie wordt beheerd, is het mogelijk om met één actie alle rechten van een gebruiker in te trekken. Erg nuttig bij bijvoorbeeld ontslag. Tevens wordt functiescheiding op een eenvoudige wijze afgedwongen. In de I AM-oplossing kan men aangeven welke taken (autorisaties op de gekoppelde doelsystemen) niet in één rol mogen worden gecombineerd en welke rollen dus niet door een en dezelfde persoon mogen worden uitgevoerd. Het koppelen van taken aan rollen en het koppelen van rollen aan gebruikers wordt Role Based Access Control (RBAC) genoemd.

Een andere belangrijke functionaliteit van I AM in relatie tot SOX is de krachtige monitoring- en auditingfaciliteit die een aantal I AM-pakketten biedt. Allereerst zijn er natuurlijk auditingfaciliteiten die vastleggen welke activiteiten door wie in het I AM-pakket worden uitgevoerd. Bijvoorbeeld het koppelen van een rol aan een gebruiker of het uitbreiden van de roldefinitie (koppeling taken aan rollen). Met deze functionaliteit kan altijd worden nagegaan over welke autorisaties een gebruiker op een bepaald moment de beschikking had en door wie

deze zijn toegekend. Een welbekend probleem is dat handmatig de autorisaties worden gewijzigd op de doelsystemen. Normaliter komt men hier pas achter na het uitvoeren van afzonderlijke autorisatiescans op de verschillende systemen. Met behulp van I AM is het echter mogelijk een continue vergelijking te maken tussen de autorisaties op de doelsystemen (Ist-situatie) en de vastgelegde situatie in de I AM-oplossing (Soll-situatie). Geconstateerde afwijkingen kunnen automatisch of na toestemming van bijvoorbeeld de lijnmanager of de security officer worden hersteld.

Het is geen kwestie van operational excellence òf 'in control', maar een kwestie van beide, met eventueel de nadruk op één van deze aspecten

Drijfveren in relatie tot de doelen van Identity & Access Management

Organisaties hebben verschillende drijfveren om I AM te implementeren. Bij een aantal organisaties zal I AM meer gedreven zijn vanuit operational excellence terwijl bij andere organisaties het streven naar 'in control' de boventoon voert. Het grote voordeel van I AM is dat het aan de realisatie van beide gebieden bijdraagt, waarbij de organisatie zelf bepaalt waar de accenten worden gelegd. Wanneer een organisatie echter alleen operational excellence nastreeft bestaat het risico dat I AM nauwelijks een bijdrage levert aan het 'in control' zijn. Door alleen de operationele autorisatieprocessen te consolideren en efficiënter uit te voeren door onder meer de toepassing van provisioning kan een organisatie namelijk al een behoorlijke stap zetten richting kostenreductie en verbetering van het gebruikersgemak. De kwaliteit van I AM kan echter alleen worden verbeterd door de herinrichting van het tactisch management en door gebruik te maken van rolgebaseerd autorisatiemanagement (RBAC). Het is dus geen kwestie van operational excellence of 'in control', maar een kwestie van beide, waarbij een organisatie kan kiezen om op één van deze aspecten de nadruk te leggen.

Op weg naar Identity & Access Management

Business case

Uiteraard moet er een positieve business case aanwezig zijn om een I AM-traject te starten. In deze paragraaf wordt kort ingegaan op de belangrijkste aspecten voor een I AM-business case. Om vast te stellen of er in uw organisatie een positieve business case bestaat, moeten de volgende drie kernvragen worden beantwoord:

1. Levert I AM een wezenlijke bijdrage aan beleidsdoelstellingen van uw organisatie?
2. Welke kwalitatieve en kwantitatieve baten kan I AM in uw organisatie realiseren?
3. Welke kosten brengt I AM eenmalig en structureel met zich mee?

Bij de beantwoording van de eerste twee vragen zal het onderscheid tussen operational excellence en 'in control' een belangrijke rol spelen. De organisatie moet aangeven op welke van de twee aspecten de nadruk wordt gelegd en op basis hiervan de kwantitatieve en kwalitatieve baten bepalen. Hierbij dient te worden opgemerkt dat de baten voor 'in control' voornamelijk kwalitatief zullen zijn en de baten voor operational excellence ook een kwantitatieve component bevatten.

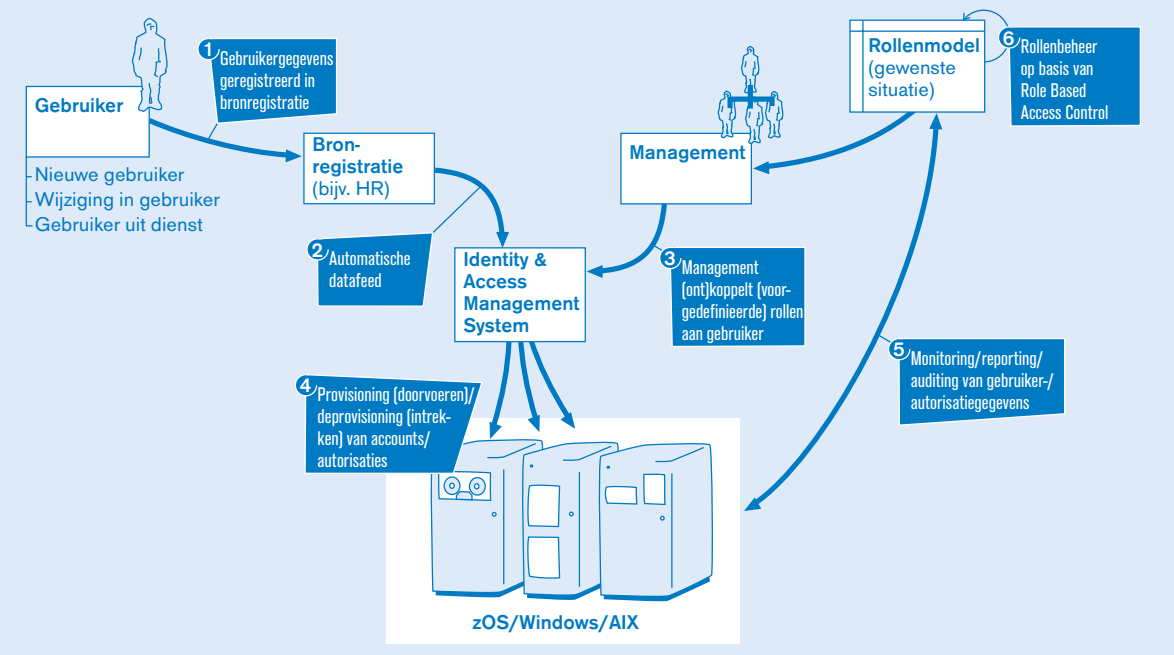
Bij het bepalen van de baten is het aan te raden om de huidige situatie in kaart te brengen, zowel in relatie tot de uitvoering van het proces als in relatie tot de kosten. Op deze wijze wordt inzichtelijk waar en waarom verbeteringen noodzakelijk zijn. Hiermee wordt de aanleiding van het project duidelijk. Daarnaast is het voor een goede inschatting van de baten en kosten noodzakelijk dat:

- de toekomstige oplossing op hoofdlijnen wordt beschreven;
- inzicht bestaat in het aantal gebruikers en het aantal vanuit het I AM-systeem te beheren doelsystemen (de scoping);
- bekend is welke I AM-processen geïmplementeerd zullen worden en dus moeten worden ondersteund door het systeem;
- de implementatiestrategie c.q. roadmap op hoofdlijnen is beschreven.

Een belangrijk aandachtspunt is dat de kosten voor de technische implementatie van I AM voornamelijk uit de licentie- en onderhoudskosten van het systeem bestaan. Het opstellen en implementeren van een gedetailleerd rollenmodel vergt, afhankelijk van de omvang van de organisatie en de diversiteit van de processen, echter ook een behoorlijke investering qua tijd en geld. Hierbij zal met name de business betrokken moeten zijn.

Blauwdruk I AM

In de blauwdruk wordt op hoofdlijnen aangegeven hoe I AM in de organisatie wordt geïmplementeerd. Hierbij wordt onderscheid gemaakt tussen het I AM-beleid, het conceptuele model en het technisch ontwerp. De blauwdruk is nadrukkelijk geen volledige uitwerking van de toekomstige implementatie, maar dient als basis om de verschillende deelprojecten van het I AM-programma verder uit te werken en te prioriteren.



Figuur 3. Generieke workflow van de I AM-processen.

Allereerst worden de uitgangspunten gedefinieerd waaraan de I AM-oplossing moet voldoen. Het informatiebeleid en het informatiebeveiligingsbeleid kunnen hierbij als uitgangspunt dienen. Omdat deze uitgangspunten vaak van een hoog abstractieniveau zijn, worden deze geconcretiseerd naar het I AM-beleid. Voor de blauwdruk is het voldoende om dit beleid op hoofdlijnen te definiëren. Aspecten die in het beleid naar voren komen, hebben onder andere betrekking op functiescheiding, te ondersteunen doelgroepen en systemen (c.q. applicaties, services en platformen), wijze van toekennen van de autorisaties (rollenmodel), authenticatiemiddelen en rapportage- en auditfunctionaliteiten. Tijdens de Proof of Concept (zie de hiernavolgende paragraaf) wordt het I AM-beleid in detail uitgewerkt.

In het conceptuele model wordt op hoofdlijnen een beschrijving gegeven van de wijze waarop de I AM-processen in de organisatie worden ingericht en welke componenten van een I AM-systeem hiervoor moeten worden geïmplementeerd. Daarbij wordt onderscheid gemaakt tussen de doelstelling van het proces, een beknopte procesbeschrijving, de beoogde functionaliteit van de I AM-component en de betrokken actoren en hun verantwoordelijkheden in het proces. Bij het definiëren van de actoren, hun betrokkenheid en verantwoordelijkheden is het aan te raden om een matrix op te stellen op basis van het zogenaamde RACI-model (Responsible / Accountable / Consult / Inform). Figuur 3 geeft een generieke workflow van de I AM-processen weer en kan als basis worden gebruikt voor het opstellen van het conceptuele model.

Het technisch ontwerp beschrijft op welke wijze het I AM-systeem wordt geïmplementeerd binnen de infrastructuur van de organisatie. Belangrijke aspecten hierbij zijn de bronregistraties (bijvoorbeeld SAP HR) en de doelsystemen waarop de in I AM aangegeven autorisaties moeten worden geïmplementeerd. De bronregistraties voeden het I AM-systeem met authentieke gegevens over de te beheren gebruikers (medewerkers, partners, leveranciers, services, etc.). Het is nadrukkelijk niet de bedoeling dat I AM een kopie van de bronregistraties wordt. Alleen de voor de I AM-processen benodigde gegevens worden geïmporteerd vanuit de bronregistraties. De doelsystemen kunnen worden ingedeeld in de volgende categorieën:

- *Systemen met een eigen authenticatie- en autorisatieadministratie*

Deze systemen authenticeren en autoriseren gebruikers op basis van data die in het systeem zelf zijn opgeslagen. Alle benodigde gegevens dienen dus in het systeem te worden opgeslagen.

- *Systemen met eigen autorisatieadministratie en externe authenticatie*

Voor de implementatie van I AM is een gefaseerde aanpak noodzakelijk

Dit type systemen voert de autorisatie op dezelfde wijze als bij het eerste type. Voor de authenticatie wordt echter gesteund op een andere, interne bedrijfsapplicatie (indien gewenst kan dit ook een externe applicatie zijn), bijvoorbeeld Active Directory. Het voordeel hiervan is dat authenticatiedata gecentraliseerd kunnen worden opgeslagen en beheerd via I AM.

- *Systemen met externe authenticatie en autorisatie*

Het systeem steunt voor de autorisatie en authenticatie volledig op een andere applicatie. Deze andere applicatie kent een elektronisch ticket toe aan de gebruiker, waarmee deze kan aanloggen op het doelsysteem.

Een ander belangrijk aspect zijn de interfaces tussen het I AM-systeem en enerzijds de bronregistratie en anderzijds de doelsystemen. Veel leveranciers van I AM-systemen hebben een aantal standaardinterfaces beschikbaar voor de koppeling met standaardsystemen. Het is hierbij van belang om aan te sluiten op internationale standaarden, zoals de Liberty Alliance, SAML, SOAP en LDAP.

Implementatie Identity & Access Management

Voor de implementatie van I AM is een gefaseerde aanpak noodzakelijk. I AM is namelijk complex, raakt alle (ICT-)resources en bedrijfsprocessen, en vereist zowel een sterke betrokkenheid van de organisatie als een multidisciplinaire aanpak. De implementatiedimensies zijn voornamelijk afhankelijk van:

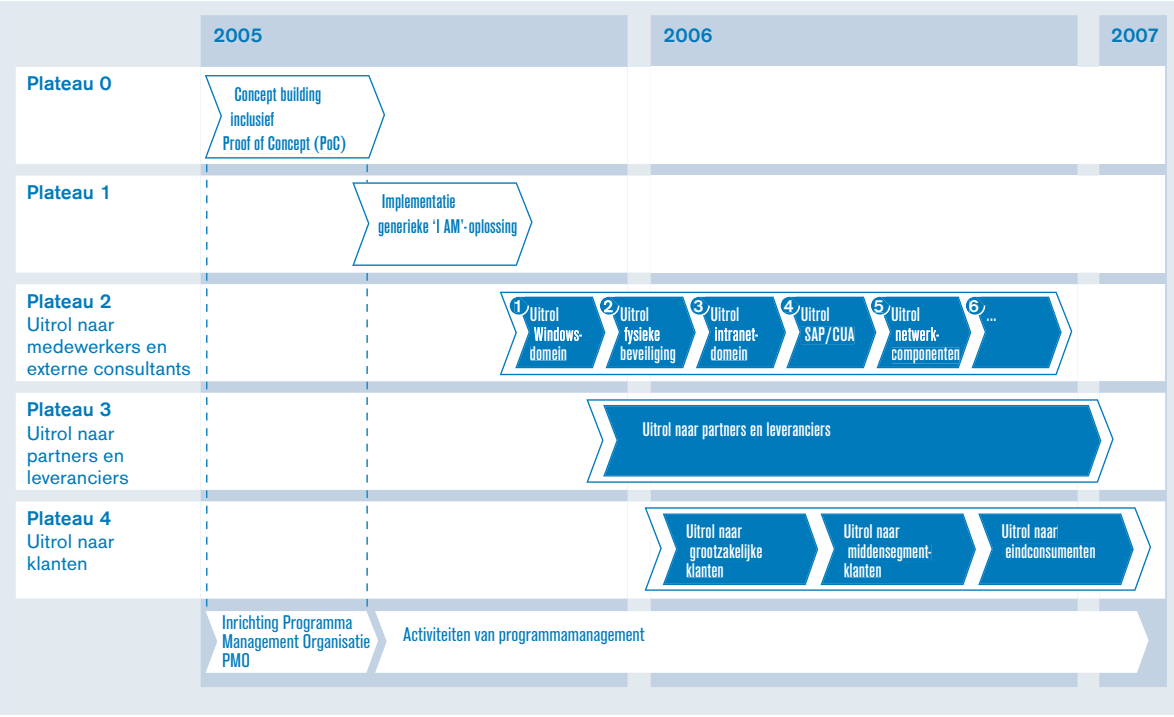
- de doelgroepen die moeten worden beheerd;
- de beoogde functionaliteit;
- de doelsystemen die moeten worden beheerd;
- de aanwezige infrastructuur;
- de organisatiestructuur.

Op basis van de bovenstaande dimensies, de business case en de blauwdruk dient een I AM-roadmap te worden opgesteld, waarin op hoofdlijnen wordt aangegeven welke fase wanneer wordt uitgevoerd. In figuur 4 is een voorbeeld van een roadmap gegeven.

Zoals uit deze roadmap is af te leiden wordt gestart met de fase Concept building, waarin een Proof of Concept (PoC) wordt uitgevoerd. In de PoC wordt in een beperkte omgeving (beperkt aantal doelsystemen en gebruikers) de I AM-oplossing geïmplementeerd. In de praktijk komt het ook voor dat de PoC onderdeel is van de leveranciersselectie. Voor de PoC kunnen bijvoorbeeld op basis van een Request for Proposal (RfP) twee of drie leveranciers worden geselecteerd die ieder één week de tijd krijgen om hun pakket te installeren en te configureren. Vervolgens wordt dan in een aantal dagen een aantal processcenario's doorlopen op basis waarvan wordt geëvalueerd of de I AM-oplossing voldoet aan de eisen en wensen van de organisatie en wordt de beslissing genomen om I AM organisatiebreed te implementeren. Hierbij spelen de volgende aspecten een belangrijke rol:

- technische inpasbaarheid;
- organisatorische inpasbaarheid;
- functionele eisen;
- bijdrage aan de in de business case geïdentificeerde baten;
- bijdrage c.q. voldoen aan het informatie- en beveiligingsbeleid van de organisatie.

Om een gefundeerde uitspraak te kunnen doen over het voldoen aan de eisen in relatie tot de bovenstaande aspecten is het van belang dat er op basis van de business case en het I AM-beleid uit de blauwdruk concrete



Figuur 4. I AM-roadmap.

evaluatiecriteria worden opgesteld waarmee kan worden getoetst of de I AM-oplossing daadwerkelijk een bijdrage levert aan de gestelde doelen. Deze criteria kunnen tevens als input dienen bij het opstellen van de RfP.

Na een positieve evaluatie kan worden gestart met de organisatiebrede implementatie van de I AM-oplossing in overeenstemming met de opgestelde roadmap. Indien met meerdere leveranciers de PoC wordt uitgevoerd, moet eerst een keuze worden gemaakt voor één leverancier.

Ten slotte is het van belang om een onderscheid te maken tussen enerzijds de selectie en implementatie van het I AM-pakket en het uitvoeren van de PoC met een eenvoudig rollenmodel en anderzijds de grootschalige uitrol met een gedetailleerd rollenmodel, zoals zal geschieden in plateau 2 en volgende plateaus. Het opstellen van een gedetailleerd rollenmodel vergt namelijk veel tijd en een intensieve betrokkenheid van de business, waarbij veel tijd gaat zitten in de afstemming van het rollenmodel. Om quick wins te behalen en om vertraging in het project te voorkomen is het daarom aan te raden om tijdens de PoC en de implementatie van het I AM-systeem slechts met een aantal generieke rollen te werken. Vervolgens kan het rollenmodel gedetailleerd worden uitgewerkt en geïmplementeerd. Een tweede optie is om wel vrij snel te starten met het rollenmodel, maar de voortgang van de PoC en de technische implementatie hier niet van af te laten hangen. Op deze wijze worden de quick wins ook behaald, omdat de generieke rollen al kunnen worden gebruikt alvorens het gedetailleerde rollenmodel is uitgewerkt.

Conclusie

Organisaties hebben verschillende drijfveren om Identity & Access Management te implementeren. Bij een aantal organisaties zal I AM meer gedreven zijn vanuit operational excellence, terwijl bij andere organisaties het streven naar 'in control' de boventoon voert, echter beide elementen zijn onlosmakelijk met elkaar verbonden. Per organisatie zal het verschillen in welke fase van het programma welk element de boventoon voert. Terugkomend op de titel van ons artikel is het dus niet operational excellence of 'in control' maar is het operational excellence & 'in control'.

Literatuur

[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.