PvIB Expertbrief – Januari 2011
ISSN 1872-4876, jaargang 7 – Nr. 2

Access management (Deel 3: Projectmanagement)

Peter Hoogendoorn

Jean-Pierre Vincent

Wiyaykumar Jharap

Piet Kalverda

Karin van de Kerkhof

Renato Kuiper

Jan-Roel Löwenthal

Henk Marsman

Danny Mol

Karel van Oort

Access management (AM) projecten zijn veelal complex. Of ze nu geïnitieerd worden vanuit een business benefit doelstelling of vanuit compliance; bijna altijd moet met betrekking tot access management een werkbare eenheid worden geschapen tussen business, compliance en ICT.
Deze expertbrief geeft de visies van de betrokken experts weer over aspecten die belangrijk zijn om een AM-project tot een succes te maken. In expertbrief 1en 2 worden reeds de AM-visie en -architectuur beschreven. Deze expertbrief beschrijft project besturingsaspecten op basis van inhoudelijke AM overwegingen. Over de wijze hoe sommige aspecten toe te passen verschillen de experts soms van mening. Kortom: deze expertbrief bevat stof tot nadenken en daarmee handvatten om overwogen beslissingen te nemen over o.a. scope, aanpak en projectinrichting voor de implementatie van AM in een voor de lezer specifieke situatie.

Pagina

2 INLEIDING EN SITUATIESCHETS

Aanleiding

Steeds meer bedrijven buigen zich over identity- en access management vraagstukken. Deze vraagstukken zijn in essentie vaak dezelfde, alleen verschillen de bedrijfssituaties en daardoor de oplossingsrichtingen. Om te voorkomen dat 'AM-wielen' opnieuw worden uitgevonden, worden deze vraagstukken door experts geformuleerd en worden aanpak- en oplossingsrichtingen uitgewerkt in 4 expertbrieven, waar deze de derde in de reeks is. Hierdoor kan de kennis op effectieve wijze worden hergebruikt.

Aanpak

Access management is complex. Het raakt immers alle medewerkers en in sommige gevallen leveranciers en klanten of partners die een relatie hebben met de organisatie op het gebied van logische en mogelijk fysieke toegangsbeveiliging. Om hiervan toch een beeld te kunnen weergeven in expertbrieven, is het onderwerp in vier hoofdgebieden opgesplitst die ieder worden uitgewerkt in een expertbrief. In Bijlage 1 is beschreven hoe deze opsplitsing is uitgevoerd.
Deze expertbrief, deel 3, behandelt de project managementaspecten rondom een access management implementatie. Om tot deze expertbrief te komen is een zogenaamd kapstokdocument opgesteld met generieke project management onderwerpen. In de werkgroep zijn deze onderwerpen besproken en hebben de betreffende specialisten hun inbreng gegeven in de uitverwerking daarvan in deze expertbrief.

Scope

De scope van deze expertbrief richt zich op access management. Identity management is buiten scope. Beiden kunnen echter niet zonder elkaar, waardoor het maken van scheiding lastig is. De expertgroep heeft geoordeeld dat het duidelijker is om aan te geven dat er geen aandacht wordt besteed aan identificatie- en authenticatie-oplossingen, beheer en controle op smartcard-oplossingen, SSO-oplossingen en mechanismes om te controleren of 'je bent wie je zegt dat je bent'. In deze expertbrief gaat de aandacht uit naar wat nodig is voor het verstrekken van autorisaties: beleid, organisatiestructuur, processen, bemensing, administratie en (technische)middelen.

Doelstelling

De expertbrief heeft tot doel een hulpmiddel te zijn bij het implementeren of verbeteren van een access management organisatiestructuur en beheeromgeving. De expertbrief formuleert per onderwerp aandachtspunten waarvan de lezer zelf kan beoordelen of deze in zijn situatie van toepassing zijn en hoe deze in zijn situatie kunnen worden toegepast.

Definitie

Meestal worden identity- en access management (IAM) in één adem genoemd omdat deze begrippen sterk aan elkaar zijn gerelateerd. Ter afbakening van het begrip access management, gebruiken we de volgende definities:

Access management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om de toegang tot en het gebruik van systemen en informatie te faciliteren, beheren en controleren.

Identity Management is het geheel aan beleid, verantwoordelijkheden, processen en hulpmiddelen dat organisaties in staat stelt om van actoren (als gebruikers en systemen) de identificatie en authenticatie te faciliteren, beheren en controleren.

Toelichting op access management:
Access management betreft het regelen van de toegang van een subject (bijvoorbeeld een medewerker, systeem, service, etc.) tot een object, bijvoorbeeld data of het gebruiken van een service. In beide gevallen moet worden vastgesteld of het betreffende subject het recht heeft om bij de databron te komen (de resource mag de data inzien of muteren[1]) of de service mag gebruiken (bijvoorbeeld: is er een licentie voor de resource beschikbaar). In een enterprise-omgeving gaat het hierbij om veel rechtenverstrekkingen en de controle daarop (schaalgrootte). Daarom loont het zich om de uitvoering daarvan efficiënt in te richten door middel van helder beleid, strakke processen, juiste bemensing met de bijbehorende verantwoordelijkheden, correcte administraties en goede (technische) hulpmiddelen.

Totstandkoming expertbrief
Deze publicatie is het resultaat van de 3e expertsessie ‘access management’ en is tot stand gekomen met medewerking van de genoemde personen op de voorpagina (zie voor meer achtergrondinformatie bijlage 2).

Initiatiefnemer van de ‘access management’ expertsessies is Jean-Pierre Vincent. Samen met Aaldert Hofman, Bart Bokhorst en Ben Elsinga is de initiële probleemstelling geformuleerd. Deze is verder uitgewerkt door het organisatiecomité.

De organisatiecomitérollen zijn als volgt ingevuld:

Probleemeigenaar:	Karin van de Kerkhof
Facilitator:	Jan-Roel Löwenthal
Co Facilitator:	Danny Mol
Ghostwriters:	Jean-Pierre Vincent en Peter Hoogendoorn

[1] Onder muteren wordt hier verstaan het creëren, verwijderen en wijzigen van data.

4

DE ONDERZOEKSVRAGEN

AM-projecten zijn complex. Ze bestrijken de hele organisatie en raken zowel de business als ICT. Onderwerpen die spelen naast de gangbare projectmanagementvraagstukken (scope, risico's, planning, resourcing) zijn:

- Top-down (van beleid naar oplossing) en/of bottom-up aanpak (door het schonen/verbeteren van de oplossingssituatie komen naar een hoger security volwassenheidsniveau) of een mix van de top-down en de bottom-up aanpak.
- Het vaststellen van de juiste oplossing (o.a. architectuur, rollenmodel, methode, tooling).
- Het implementeren van de governacne van access management .
- Het in de business uitrollen van nieuwe autorisatiemodellen, AM-verantwoordelijkheden, AM-processen, AM-tooling, etc.

De basis van deze expertbrief is de vraag hoe je zo goed mogelijk met deze onderwerpen om kunt gaan bij het inrichten en het uitvoeren van een AM-project. Om de vraagstelling scherp te krijgen is onderstaande probleemstelling geformuleerd.

Probleemstelling voor de expertbrief 'Het Access Management implementatie project'

Voor deze expertbrief zijn de volgende vragen geformuleerd omtrent AM-implementatie-projecten:

- **Projectaanpak:** kunnen de organisatorische projectaspecten zowel vanuit een klassieke (waterval) als vanuit een flexibele methodiek worden benaderd?

- **Projectorganisatie-inrichting:** welke resources dienen vanuit de business en ICT-afdelingen te worden betrokken? Welke projectmandaten zijn nodig om het project succesvol te kunnen laten zijn?

- **Projectproducten en -fasering:** welke producten worden opgeleverd? Welke instrumenten worden gebruikt? Welke hulpmiddelen zijn nodig? In welke volgorde kunnen activiteiten worden uitgevoerd en welke projectfasering past daar bij (zie voorbeeld figuur 1)? Welke aspecten lenen zich het beste als 'quick-win' op welk moment?

- **Aanpak en implementatie:** wat zijn de voor- en nadelen van aanpakken als bottom-up, top-down of werkt ook een mix van beide? Hoe worden ontwerp en bouw van de producten aangepakt? Hoe voer ik aanpassingen door in de lijnorganisatie en hoe beleg ik nieuwe autorisatieprocessen in de organisatie? Hoe vindt in de business de migratie naar een nieuw/centraal autorisatiemodel plaats, bijvoorbeeld: draagt "role-mining" daadwerkelijk iets bij, hoe word een nieuw autorisatiemodel geadministreerd (bijvoorbeeld rollen, rules, entitlements, etc.), hoe wordt de provisioning opgezet? Hoe en wanneer wordt het operationeel beheer van de nieuwe of verbeterde AM-voorzieningen overgedragen aan de AM beheerorganisatie in de lijnorganisatie?

Deze onderwerpen zullen worden onderzocht op hoe deze optimaal kunnen worden opgezet/ingericht in een AM implementatieproject en welke aspecten daarbij belangrijk zijn. Ook worden valkuilen en projectrisico's beschreven. Zie ook het hoofdstuk 'Lessons learned'.

N.B. In deze expertbrief wordt niet ingegaan op het toepassen van een specifieke projectmethodiek als Prince2, MSP, etc. De onderwerpen worden generiek besproken en kunnen in alle projectmethodieken worden toegepast.

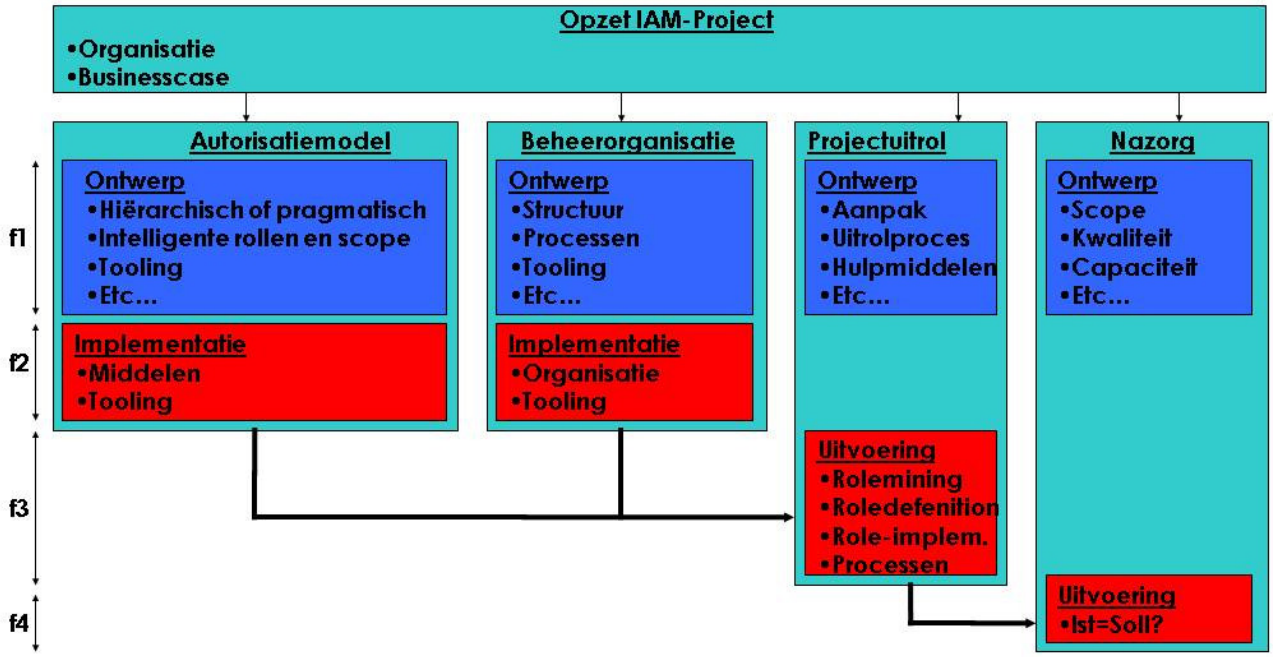


Fig. 1. Een eenvoudig voorbeeld van een AM-projectstructuur en -fasering.

Figuur 1 geeft slechts een invalshoek vanuit de processen en techniek weer, uiteraard spelen de verandermanagementaspecten in het project een grote rol.

Samengevat zijn de uitgangspunten van de sessie de volgende vragen:

1. Bestaat er een optimale aanpak voor AM-projecten?
2. Welke bevoegdheden en resources zijn nodig in een AM-project?
3. Hoe is een AM-project te faseren en welke producten zijn te benoemen?
4. Welke werkwijzen en tips voor doorvoeren van de wijzigingen in de organisatie kunnen worden verstrekt?
5. Hoe vindt de overdracht naar beheer plaats?

6

BESTAAT ER EEN OPTIMALE AANPAK VOOR ACCESS MANAGEMENT PROJECTEN?

Is er een ideale aanpak en komen altijd dezelfde projectelementen en vraagstukken terug?

Een ideale projectaanpak die in alle gevallen tot een succes leidt is voor een AM-project niet te geven. Daarvoor is de problematiek te ingewikkeld. Wel geldt als uitgangspunt dat de probleemeigenaar van autorisaties de business is en niet IT. Het project dient daarom ook vanuit de business gestart te worden.

Er is een aantal projectelementen die steeds terugkeren. Deze zijn hieronder uitgewerkt:

- Context:
    - De project opdrachtgever met zijn / haar belangen.
      Het doel dat de opdrachtgever beoogt, geeft aan welke sturing benodigd is (vragen als centraal/decentraal, financiering, scoping en ambitie spelen hier een hoofdrol).
    - In welk domein van de organisatie het project wordt uitgevoerd (IT/Business/ Risk/Legal/etc); een AM-project in de IT-omgeving vraagt om aandacht voor technische koppelingen en aandacht voor beheer, in de business vraagt het om redenen waarom een medewerker bepaalde autorisaties moet hebben, bij Security/Risk vraagt het om afstemming wat ‘in-control’ zijn betekent en hoe dat uitvoerbaar is te maken. Deze doelen per domein, dienen in de projectdeliverables en de fasering (dus in de uitrolstrategie) van het project tot uitdrukking te komen.
    - De scope van het project en de betrokkenheid van de business / lijnorganisatie; Betreft het alle systemen / medewerkers / externe partijen / processen van de organisatie of slechts een deel daarvan en op basis waarvan wordt dit vastgesteld?
- Businesscase: de initiële businesscase met de reden waarom we AM willen doen en wat de benefits zijn. Om een businesscase op te stellen is het mogelijk zinvol om een ‘Proof Of Concept' (POC) uit te voeren. Hier kan duidelijk worden hoe complex de gewenste koppelingen zijn (bijv. HR, Active Directory) en of de bedachte workflows goed werken. Stel vast dat de efficiency winst ook inderdaad gehaald kan worden (transparantie en meetbaarheid van de businesscase) en waar problemen kunnen optreden die eerst opgelost moeten worden voordat je bedrijfsbreed gaat invoeren. Een voorbeeld hiervan in de praktijk is dat het toewijzen van eigenaarschap (van applicaties, AM-processen, etc.) tot veel discussies lijdt en daarmee tijd kost (terwijl het een belangrijke randvoorwaarde is voor goed autorisatiebeheer), het doorvoeren van classificatie gebeurt vaak zeer subjectief en leid tot discussie tussen applicatie-eigenaren en Risk Management, etc.. Door voor dergelijke onderwerpen een separate businesscase te formuleren, wordt het nut van deze onderwerpen inzichtelijk en kan dit helpen bij het prioriteren hiervan.
- Specificaties: het bepalen van de businesseisen ten aanzien van access management, dit zijn businessvereisten in termen van wat de organisatie wil bereiken met access management en op welke omgevingen men deze wil toepassen. Daarnaast is het van

belang doelgroepen te onderscheiden waarvoor een specifiek life-cyclemanagement van autorisaties geldt (business, functioneel en technisch beheer). Neem deze groepen mee bij het bepalen van de specificaties. Dit geldt ook voor partijen waaraan ICT taken en ICT beheerzaken zijn gesourced. Houd daarbij rekening met contracten/SLA's. Het doorvoeren van koppelingen naar doelsystemen (bij de sourcing partij) kan een behoorlijke impact hebben op de gesourcete werkzaamheden en/of de sourcingpartijen staan de koppelingen niet toe.

- Project Plateaus: vanuit de businesscase en de specificaties wordt een indeling gemaakt in plateaus waarin stapsgewijs de AM-omgeving qua organisatie, processen en techniek wordt geïmplementeerd. Deze plateaus worden zo gekozen dat er al vrij snel zichtbare resultaten (quick-wins) behaald kunnen worden en dat de business al direct voordelen gaat zien van de AM die gefaseerd ingevoerd wordt. Dit heet 'als project doelbewust zichtbaar zijn'. De plateau-indeling zal vooral bepaald worden door de belangrijkste business-benefits voor AM: risicomanagement, agility, efficiency (voor de business en beheer) en compliancy.

- Architectuur: het definiëren van de gewenste doelarchitectuur (SOLL) die de organisatie in 3 tot 5 jaar wil behalen met daarin inzicht in de huidige architectuursituatie (IST) en de tussenstappen (migratiearchitecturen) die per plateau gerealiseerd moeten worden om de doelarchitectuur te behalen. Die tussenstappen zorgen er tevens voor dat ook op de kortere termijn al resultaten worden geboekt. Op basis van deze AM-architectuur bestaande uit:
  - De benodigde processen voor AM.
  - De benodigde organisatorische ophanging en verantwoordelijkheden.
  - De doel informatie architectuur, waaronder een autorisatiemodel, een catalogus van autorisaties en een goedkeuringsadministratie van de aanvragen.
  - De benodigde technologie.

  worden PSA's (Project Start Architecturen) gedefinieerd voor elk plateau. De bouwstenen (Business bestaande uit: Organisatie, Processen, Diensten, de Informatie-architectuur bestaande uit: Applicatie en Gegevens en de Techniek bestaande uit: Middelware, Platformen en Netwerken) die benodigd zijn, zijn grotendeels behandeld in de 2e expertbrief access management (architectuur). In die expertbrief zijn componenten benoemd die in samenhang en volgordelijkheid op basis van de benoemde plateaus uit de visie en het beoogde AM-volwassenheidsniveau gerealiseerd moeten worden.

- AM-project: dit project realiseert via deelprojecten en een standaard projectmethodiek, zoals PRINCE2, de plateaus en definieert voor elk plateau een AM-project. Elk AM-deelproject zal door middel van een PID (Project Initiatie Document) en een PSA (Project Start Architectuur) aangestuurd worden. Na de realisatieprojecten zal het project ook veel aandacht moeten besteden aan de zachte kanten van de invoering van AM, namelijk: awareness en cultuur. Dit is het verandermanagement-deel van een AM-project. De business speelt hier een belangrijke en sturende voorbeeldrol.

8

Aan de hand van een tweetal scenario's wordt op basis van bovenstaande een "optimale" projectaanpak geschetst:

Scenario 1:

Voor auditors is autorisatiemanagement een geliefd aandachtsgebied. Bijna altijd valt er wel wat op te merken over het niet volledig op orde zijn van verstrekte autorisaties. Het scenario is dan ook dat in een bedrijfsonderdeel op autorisatiegebied auditbevindingen zijn gerapporteerd.

Kenmerken:

Een auditbevinding heeft altijd een vastgestelde scope (een afdeling, business unit). Het doel is duidelijk, namelijk zoals gesteld in het auditrapport.

Mandaten:

Opdrachtgeverschap ligt idealiter bij de business en wordt gedelegeerd belegd bij de information security manager.

Vanuit IT/Risk/Legal wordt input gegeven, maar geen sturing, met duidelijk afgebakende deelopdrachten, in lijn met de expertise:

1. IT – (on)mogelijkheden van de applicatie.
2. Risk: vanuit een risicobenadering evenwicht brengen in autorisatiemaatregelen en operationele maatregelen in lijn met de risk-appetite.
3. Eventuele competence centers brengen hun input in.
4. Legal: wettelijk opgelegde normen als input voor autorisatie elementen.
5. Beheer: streven naar minimale beheerlast.

Fasering:

Er ligt een auditrapport dat de focus bepaald, de inventarisatie van de huidige situatie kan daarmee tot een minimum worden terug gebracht.

1. Inventarisatie knelpunten, beschouwen huidige situatie en inbreng van expertise.
2. Samen met business kijken naar businessprocessen, mogelijke alternatieve organisatie indeling, output is hier een geactualiseerde procesbeschrijving.
3. Met rollenbeheerders vaststellen van de vereiste rollen, proefdraaien met de business.
4. Test fase.
5. Oplevering.

Scenario 2:

Vanuit een 'greenfield' situatie inrichten van AM. Er ontstaat een nieuwe situatie met sterk veranderde bedrijfsprocessen of de transitie naar bedrijfsprocessen of -ketens. In deze situatie is het veranderen vanuit de bestaande situatie vaak lastig. Een 'greenfield'[2] benadering kan dan uitkomst bieden.

Kenmerken:

Scope is hier een afdeling, business unit of een bedrijfsproces.

Duidelijk doel, op basis van nieuwe proces- en organisatie inrichting.

Mandaten:

[2] De term Greenfield is hier gebruikt om een bewuste scheiding tussen oude en nieuwe situatie te definiëren waarbij vanuit een compleet nieuwe invalshoek wordt geredeneerd waarbij het essentieel is barrières uit het verleden geen prominente rol te laten spelen.

Opdrachtgeverschap idealiter vanuit de business, gedelegeerd belegd bij de information security manager.
Input maar geen sturing vanuit IT/Risk/Legal met duidelijk afgebakende deel opdrachten in lijn met de expertise:

1. IT – (on)mogelijkheden van de applicatie, dit is nu niet meer een gegeven maar er kan vanuit requirements worden geredeneerd.
2. Risk: vanuit een Risico benadering evenwicht brengen in autorisatie maatregelen en operationele maatregelen in lijn met de risk-appetite. Dit kan nu veel meer vanuit requirements dan vanuit een bestaande situatie.
3. Eventuele competence centers brengen hun input in.
4. Legal: wettelijk opgelegde normen als input voor autorisatie elementen.
5. Beheer: streven naar minimale beheerlast en optimale indeling van autorisatie maatregelen en mogelijk application controls.

Fasering:

Er liggen requirements vanuit risico aandachtsgebieden; kernpunt hier is niet teveel in de 'oude' denkpatronen te vervallen maar echt vanuit de nieuwe situatie te denken.

1. Opstellen requirements. Hier is leunen op de expertise in competence centers belangrijk alsmede het toetsen bij een onafhankelijke klankbordgroep.
2. Samen met business kijken naar businessprocessen, mogelijke alternatieve organisatie indeling. Output is hier een optimale procesbeschrijving met daarin gelijk meegenomen hoe aan de opgestelde requirements wordt voldaan.
3. Met rollenbeheerders vaststellen van de vereiste rollen, proefdraaien met de business. Hier kunnen ook de beheerprocedures optimaal worden ingericht.
4. Test fase.
5. Oplevering.

GESTELD KAN WORDEN DAT EEN AM-PROJECT OF -PROGRAMMA IN FEITE NIETS ANDERS IS DAN EEN "REGULIER" PROJECT OF PROGRAMMA, WAARBIJ MET NAME DE INHOUDELIJKE STURING OP DE TE REALISEREN COMPONENTEN (TECHNIEK, ORGANISATIE EN PROCESSEN) OP EEN PLATEAU ACHTIGE WIJZE GEÏMPLEMENTEERD MOET WORDEN WAARBIJ DE AM-VOLWASSENHEIDSBEHOEFTE MOET MEELOPEN MET DE VOLWASSENHEID VAN DE INFORMATIEBEVEILIGING.

10 PROJECT ORGANISATIE INRICHTING

Centraal staat de vraag: Welke bevoegdheden en resources zijn nodig in een AM-project?

Het opzetten van een projectorganisatie kent een aantal standaard elementen die voorgeschreven zijn door de gekozen projectmethodiek. In deze paragraaf worden de specifieke inrichtingskenmerken van een AM-project beschreven aan de hand van de onderwerpen “bemensing”, “project opzet”, “Scoping” aangevuld met “Mandaat”.
Omdat AM voornamelijk een business aangelegenheid is maar een dergelijk project toch vaak in de marge van de onderneming wordt geplaatst (Je maakt immers geen nieuwe producten, genereert geen nieuwe klanten), is het beschikken over mandaat erg belangrijk.

Bemensing

Wat valt in zijn algemeenheid te zeggen over de projectbemensing, hiërarchie, project board in relatie tot de business en de IT-wereld?

Vooraf enkele opmerkingen:
Het is afhankelijk van de scope en reikwijdte van het project en de volwassenheid van de organisatie welke inrichting optimaal is. Projectleden moeten beseffen dat een AM-project geen ‘technology-only’ project is. Het moet door de business gestuurd/gedreven worden in balans met de technische (on)mogelijkheden en conform het beleid zoals door Riskmanagement is bepaald. Idealiter komt de drive vanuit de business. Niet risk management, security of compliance. Risk management is voor de business wel een driver om de risico's te beheersen! Dit zijn wel sponsors, maar geen drivers omdat het dan als een ‘moetje’ wordt gezien en niet als essentieel voor de business. In de praktijk zien we ook dat de business zich steeds meer bewust is van het belang van riskmanagement (het ‘in-control zijn’, het belang van voldoen aan wet- en regelgeving en functiescheiding) en dus van AM.

Hieronder volgt een indeling met daarbij de gewenste bemensing:

Een stuurgroep:
Dit betreft een sturende eenheid waaraan de programmamanager verantwoording aflegt en bestaat uit:

- Business vertegenwoordiging (CEO-opdrachtgeverschap).
- ICT vertegenwoordiging (CTO/CIO rol) als leverancier.
- HR/CRM vertegenwoordiging als leverancier (opmerking: CRM voor het geval autorisaties van de klantdoelgroepen ook als scope wordt meegenomen).
- Information security Officer rol (tevens als gebruikersrol).
- AM-programmamanager.

Een klankbord groep:
Deze groep controleert aspecten als kwaliteit, risico’s en business benefits en bestaat uit:

- Experts vanuit de business domeinen.
- Informatiemanager, ICT architect, Technisch- en Functioneel applicatie beheerder (TAB/FAB) domein applicaties.
- Auditgroep/ interne controle voor bewaking normenkaders.

Een ontwerp, architectuur & beleids projectgroep:
Deze groep verzorgt de relatie van beleid naar maatregelen en oplossingen. Tevens beschrijft deze groep de governance inrichting, het functioneel ontwerp en projectzaken als de projectaanpak voor de uitrol in de business. Deze groep bestaat uit:

- Projectmanager;
- Business experts vanuit de betrokken business domeinen die hun verantwoordelijkheid nemen in het (deel)project behorende bij hun domein;
- Business architect;
- Communicatie specialist (denk aan nieuwsbrieven en allerlei communicatie die noodzakelijk is);
- AM-architect (zie ook AM-expertbrief 1 en 2);
- Security (CISO) Corporate Information Security Officer- en (SM) Security Manager-rol;
- Autorisatiemodel-specialisten (zie ook AM-expertbrief 2);
- AM-specialisten.

Een technische projectgroep:
Deze groep richt zicht op het selecteren van een juiste oplossing, het beschrijven van het technisch ontwerp, het testen en implementeren van de oplossing, de groep bestaat uit:

- Technisch projectleider;
- ICT: Ontwerpers, bouwers, testers;
- Beheerders (TAB- Technisch Applicatie Beheer, FAB- Functioneel Applicatie Beheer) van de aan te sluiten systemen;
- Ondersteuning door leverancier in verschillende rollen.

Een Kenniscentrum:
Bij grotere omvang van het project is het handig om een kenniscentrum AM op te richten die de benodigde operationele expertise heeft en/of opdoet en eventueel centraal beschikbaar stelt.
Binnen deze groep wordt ook op basis van de beschreven governance inrichting de AM-processen beschreven en geïmplementeerd. Wanneer het AM-project impactvolle wijzigingen in het dagelijks werk tot gevolg heeft voor bijvoorbeeld beheerders, worden inhoudelijke functieaanpassingen afgestemd met HR en de OR. Eventuele gebruikersparticipatie kan vanuit deze groep goed geregeld worden.

- Technische expertise;
- HR expertise;
- AO expertise
- (AM-) Proces architect (zie ook AM-expertbrief 2);
- Opleidingsexpertise om toekomstige rollenbeheerders of autorisatiebeheerders op te leiden. Betrek deze ook gelijk bij het project;
- Beheer expertise, zoals toekomstige autorisatiebeheerders of rollenbeheerders.

In deze groep is het belangrijk overzicht te hebben over onderlinge afhankelijkheden zoals:

- De afhankelijkheid van HR procedures.
  De rol van HR is belangrijk omdat bij wijzigingen van HR-procedures, dit direct invloed heeft op de AM processen.
- Regie functie op outsourcingspartijen.
  Zorg ervoor dat de regie over uitbestede processen en software leveranciers in eigen hand wordt gehouden

Het kennis centrum kan prima worden bemand door de huidige beheerorganisatie. Dit is een ideaal concept omdat daarmee de overgang van huidige werkwijze en nieuwe werkwijze binnen dit gremium gerealiseerd wordt. Het antwoord op de vraag omtrent 'overdracht naar beheer' wordt dus hier gegeven. Breng in het kenniscentrum de huidige centrale beheerorganisatie onder.

Lokale of decentrale projectgroep:
Deze groep realiseert de lokale business implementatie.

- Deelprojectleider;
- Directielid als sponsor mogelijk in mini stuurgroep (ook hier liefst gedreven vanuit een duidelijke business behoefte);
- Risk management, locale security officer/manager;
- Business process managers/ ontwerpers;
- Business architecten;
- Beheerders (FAB, TAB) van lokaal beheerde systemen.;
- Gebruikers;
- Mogelijk een externe consultant voor inbreng expertise en een onafhankelijke partij voor het bieden van ondersteuning bij conflicten.

Project opzet

Welke deelprojecten zijn voor de hand liggend, denkend aan governance inrichting (beleid en beheer), techniek die vastgesteld, uitgewerkt en geïmplementeerd moet gaan worden, schoning en de uitrol in de business?

Deelprojecten die voor de hand liggen bij een AM programma zijn:

- Project strategie: stelt de visie en roadmap voor de langere termijn op en bewaakt de alignment en de voortgang hierop van de deelprojecten.
- Project organisatie: regelt de benodigde organisatie in met de verantwoordelijkheden voor het beheer en controleren van de autorisaties en permissies.
- Project communicatie: regelt dat alle doelgroepen van de juiste informatie worden voorzien en dat het programma zichtbaar is voor de business.
- Project processen: definieert en implementeert de AM-beheerprocessen en sluit aan bij de andere beheersprocessen in de organisatie zoals security management en identiteitenbeheer, alsmede de life-cycle processen (in-, door- en uitstroom van medewerkers, de implementatie, mutatie en uitfasering van systemen, etc.), riskmanagementprocessen, etc..
- Project techniek: deze draagt zorg voor de mogelijke selectie van tooling op basis van de functionaliteit en regelt de technische aansluiting van de tooling aan de bronsystemen en doelsystemen die in de architectuur benoemd zijn. Bij enige omvang van applicaties zou je dit per applicatie als deelproject kunnen inrichten.
- Project veranderen: deze zorgt voor de awareness en de benodigde cultuur-veranderingen om AM goed te laten werken in alle domeinen van de organisatie.

Scoping

Hoe stellen we de scope vast en houden we deze zodanig dat het project beheersbaar blijft en doelstellingen gehaald kunnen worden?

De scope wordt vastgesteld met de opdrachtgever en deze wijzigt daarna niet meer. Hoewel het soms zeer aantrekkelijk lijkt om ook andere problemen die buiten scope waren op te lossen, wijst de ervaring uit dit pertinent niet te doen. Als de scope wijzigt mislukt het AM-project vrijwel zeker. Scope wijzigingen zijn wel mogelijk maar moeten als een reguliere project RFC (Request For Change) behandeld worden, waarbij de impact en de plateauplanning en ambities goed bewaakt moeten worden. Houd de scope per plateau klein en realistisch. Neem eventuele additionele wensen op in uitbreidingen voor een later te plannen plateau. Het succes van een AM-project ligt in het maken van kleine concrete stapjes.

Stel de scope samen aan de hand van een centrale businesscase en bepaal de fasering aan de hand van deze businesscase geaccordeerd door de CEO.

Van invloed op deze scoping zijn de visie en plateaus uit de AM-architectuur. Hanteer deze als uitgangspunt voor de projectaanpak zodat de stuurgroep kan toezien dat de verschillende gedefinieerde plateaus gehaald worden en beperkt blijven tot de afgesproken scope. Let op: ook bij wijzigingsverzoeken staat steeds weer de businesscase en de AM-architectuur centraal.

Afhankelijk van de situatie kan het raadzaam zijn het aantal systemen/applicaties in eerste opzet beperkt te houden maar wel een zo groot mogelijke groep gebruikers erbij te betrekken. Een geschikte keuze is altijd het primaire platform. In deze eerste opzet past ook het beperken van afhankelijkheden door het aantal interfaces te minimaliseren.

Wanneer het AM-project de uitrol van een op rol (RBAC) gebaseerd autorisatiemodel bevat, is een eerste uitrol in een service center sterk aan te raden. Veel medewerkers die hetzelfde werk doen met een beperkt aantal rollen én een hoge business benefit met betrekking tot de effecten van een snelle autorisatieverstrekking omdat de doorstroom in een dergelijke werkomgeving relatief hoog is. Uit een eerste pilot kunnen de eerste fouten gehaald worden en getuned worden aan beleid, procedures en techniek.

Project bevoegdheden en mandaat

Het AM project is een organisatie veranderproject. Beleid wordt (wellicht) aangescherpt en strak doorgevoerd, de AM-beheerorganisatie aangescherpt/vernieuwd, eigenaren aangewezen, autorisaties geschoond, etc.. De projectgroep moet daarbij voldoende mandaat hebben om deze veranderingen te kunnen doorvoeren. Het veranderen van bedrijfsprocessen, zodanig dat daarvan rollen zijn af te leiden, kan ingrijpend zijn en alleen met voldoende mandaat kan dit succesvol worden uitgevoerd. Het mandaat moet ook toereikend zijn om de werkwijze en houding van leidinggevenden te kunnen veranderen. Zie bijvoorbeeld ook de mandaatrollen zoals beschreven in de scenario's.

De veranderingen die nodig zijn in de technische omgeving dienen ook met voldoende mandaat te worden uitgevoerd. De invoering van bijvoorbeeld een centrale autorisatie-

administratie en of een directe koppeling tussen het access management systeem en de applicatie kan ingrijpende gevolgen hebben voor het werk van functioneel-, technisch- en/of autorisatiebeheerders.

Projectbeleid

Als gevolg van de complexiteit en reikwijdte van AM-projecten zijn binnen een organisatie al snel verschil van inzichten over scope, doelstelling aanpak- en oplossingsrichtingen (bijvoorbeeld een type autorisatiemodel). Het is daarom essentieel bij de start van een AM-project met alle gelederen van het bedrijf hierover afspraken worden gemaakt. Dit projectbeleid moet helder worden beschreven en gecommuniceerd.

In principe is dit een onderdeel welke thuis hoort in de architectuuruitgangspunten van een project en zou dit onderwerp eigenlijk thuis horen in de expertbrief AM-architectuur (nr. 2). In de praktijk zien we echter dat deze punten vaak net te weinig aandacht krijgen (is dus een belangrijke valkuil), waardoor discussies te laat worden gevoerd en aanzienlijke vertraging ontstaat. Derhalve noemen we de punten hier in deze expertbrief, ook omdat het niveau van de genoemde punten zich niet altijd op architectuurniveau bevinden.

Bij het opstellen van een beleidsbeschrijving moeten de volgende onderwerpen worden overwogen en worden beschreven indien van toepassing.

Aandachtspunten voor projectbeleid:

Nr	Omschrijving
PB1	Binnen het project moet in het projectbeleid helder worden gesteld hoe en door welk gremium **beslissingen** worden genomen. In dit gremium zitten eigenaren en vertegenwoordigers van de verschillende doelgroepen. Met name een representatieve vertegenwoordiging van de business is hierin een eis.
PB2	Het projectbeleid geeft aan wat het **mandaat van het project** is en hoe discussies kunnen worden voorgelegd aan bovengenoemd gremium (escalatieproces). Dit is op zich een algemeen projectmanagement aspect. Toch nemen we het op in deze expertbrief omdat het mandaat van AM-projecten soms ver kan gaan. Bijvoorbeeld wanneer beheerders van systemen moeten meewerken om 'hun systeem' volledig te voorzien van automatic provisioning, waardoor hun eigen werk overbodig wordt.
PB3	In het projectbeleid is aangegeven wat het **mandaat** is van de betreffende **projectboardleden**. Deze dient zodanig te zijn dat geformuleerde doelstellingen daadwerkelijk kunnen worden behaald en dat discussies snel met de juiste personen kunnen worden gevoerd en beslissingen snel kunnen worden genomen. Omdat er veel verschillende disciplines mee moeten werken is dit mandaat bijzonder belangrijk.
PB4	Het project moet regelen dat **eigenaarschap** van bedrijfsprocessen, services, objecten, data, informatiesystemen, applicaties en netwerken wordt **belegd** en dat zij hun verantwoordelijkheid nemen met name in de autorisatiebeheerprocessen.
PB5	In het projectbeleid moet de **medewerker scope** van het AM-project worden aangegeven. Dat is op zich een standaard projectmanagement aspect, maar wordt hier als checklist opgenomen. Deze checklist betreft:

	• Interne medewerkers; • Externe medewerkers; • Gesourcete medewerkers; • Medewerkers van externe partijen die toegang hebben op de systemen; • Klanten; • Partners; • Leveranciers.
PB6	In het projectbeleid moet de **systeemscope** van het project worden aangegeven welke systemen worden meegenomen in de nieuwe AM organisatie-inrichting. Dat is op zich een standaard projectmanagement aspect, maar het is een onderwerp die in de praktijk vaak tot discussie leidt. Bijvoorbeeld de eigenaar van een systeem waarin nauwelijks autorisatiemutaties worden doorgevoerd en die geen kritische data bevat, zal vragen waarom zijn systeem in scope van het programma is.
PB7	Het projectbeleid geeft aan **hoe** wordt **getoetst** dat gemaakte ontwerpen en de daadwerkelijke uitwerking overeenkomen met het bedrijfsbrede securitybeleid. Dat is op zich een standaard projectmanagement aspect, maar in de praktijk zien we dat het toepassen van beleidsregels verschillend wordt geïnterpreteerd en dat discussies hierover te laat worden gestart.
PB8	In het projectbeleid moet de **accountscope** van het project worden aangegeven m.b.t: • Medewerker-accounts; • Gast-accounts; • Groeps-accounts; • System-accounts. Bepaald moet worden of accounts die lang niet meer gebruikt zijn of lang inactief zijn, mogen worden ingetrokken.
PB9	Beleid moet aangeven hoe de invulling van een **autorisatiemodel** moet worden vastgesteld: • Top-down: autorisaties vaststellen vanuit de theorie. • Bottom-up: zoals de praktijk nu is. • Combinatie van beide (eerst theoretisch vaststellen en controleren in de praktijk).
PB10	Indien bedrijfsbeleid geen richtlijnen geeft voor te hanteren **frameworks en referentieconcepten**, dienen deze binnen de projectscope te worden vastgesteld. Dat is op zich een standaard architectuuronderdeel in een project, maar wordt hier specifiek genoemd, omdat in de praktijk niet altijd concrete richtlijnen worden gehanteerd, maar zelf bedachte die vervolgens weer tot discussie leiden.

PROJECTKOSTEN

De projectkosten dienen te worden gecalculeerd conform de gehanteerde projectmethodiek. Toch worden onderstaande kostenaspecten meegegeven:

PK1	Het betrekken van de business bij het opstellen en testen van rollen heeft een gunstige invloed op de acceptatie, juistheid en volledigheid van het definiëren van rollen. Het verhoogt het draagvlak vanuit de business. Hierdoor wordt dan wel een aanzienlijke inspanning van de business gevraagd die o.a. ten koste gaat van productiecapaciteit. Deze kostenpost kan worden beperkt door met architecten en analisten zoveel

	mogelijk top-down (op basis van kennis en theorie) voorbereidingswerk te verrichten voordat de business wordt betrokken. Met de business kan deze vervolgens met een bottom-up methode (wat heeft men nu aan verstrekte autorisaties en waarom) worden nagelopen.
PK2	Doelsystemen waarin veel autorisatiemutatie wordt verricht kunnen direct op de centrale autorisatie/tooling worden aangesloten (provisioning). Overweeg welke doelsystemen je wilt voorzien van automatische provisioning. Wegingsfactoren zijn: • Is het systeem bedrijfskritisch; • Is het systeem toekomstvast; • De hoeveelheid mutaties/gebruikers; • De benodigde inspanning voor het maken van de koppeling; • De kosten om het doelsysteem aan te passen.

PROJECTRISICO'S

Zoals eerder al is aangegeven zijn AM-projecten complex. Als de doelstelling is om een 'in-control'-statement te kunnen geven over de gehele organisatie, dan bestrijkt de scope van een AM-project de hele organisatie; dus: alle medewerkers, klanten, leveranciers, alle systemen, alle autorisaties. Deze complexiteit brengt een aanzienlijke hoeveelheid projectrisico's met zicht mee. Onderstaande tabel geeft projectrisico's weer die uit ervaring zijn opgedaan met een daarbij behorende aanpak- of oplossingsrichting.

Nr	Omschrijving
PR1	De aanloopfase van een project neemt veel doorlooptijd in beslag. Dit kan ogenschijnlijk leiden tot het uitblijven van resultaten. Plan ruim tijd hiervoor in. Voor een grote organisatie (> 10.000 medewerkers) is een jaar een aardige richtlijn. Stem tussentijdse resultaten helder af. De implementatie kan bij een goede voorbereiding relatief snel geschieden.
PR2	Door de lange aanloopperiode worden de businessbenefits pas laat bereikt. Dit kan leiden tot ongeduldige projectboardleden en stakeholders. Neem dit mee in het verwachtingsmanagement en ga na of het mogelijk is om gefaseerd deelresultaten op te leveren, zodat zichtbare voortgang wordt getoond. Begin pas met uitrollen in de operationele business als ook op redelijke termijn de eerste zichtbare resultaten voor hen gerealiseerd kunnen worden.
PR3	Tijdens de aanloopfase worden gaande weg vaak nieuwe stakeholders betrokken. Ook ontstaan er gedurende die periode regelmatig nieuwe inzichten. Bij een starre planning en te strak gedefinieerde projectproducten, ontstaat onvrede bij de stakeholders. Pak dit als volgt aan: Inventariseer in zo vroeg mogelijk stadium de behoefte van de stakeholders en maak het sprekend door praktische voorbeelden. Richt het project iteratief in m.b.t. de productontwikkeling en realisatie. Voer een strak project RFC beleid en hanteer een duidelijk en strak RFC proces.
PR4	Een AM-project kan veel problemen oplossen. Hierdoor ontstaat de verleiding om meer zaken in het project op te nemen dan in de eigenlijke startdoelstelling was

	vastgesteld. Voorbeelden zijn: het realiseren van een kosten doorbelasting methodiek op basis van het aantal verstrekte autorisaties, het opnemen van allerlei SLA-aspecten die gericht zijn op continuïteitsvraagstukken, etc.. Het is de kunst om een project 'klein te houden' en in eerste instantie alleen die doelstellingen na te streven die direct gerelateerd zijn aan access management.
PR5	Door het centraliseren van processen en beheertaken, veranderen de werkzaamheden van bijvoorbeeld beheerders die zich bezighouden met het verstrekken van autorisaties. Vooral bij oudere medewerkers, die al lang bij het bedrijf werkzaam zijn, kan dit leiden tot weerstand. Beschrijf zorgvuldig de nieuwe organisatie-inrichting (processen, taken en verantwoordelijkheden) en stel vast wat de consequenties zijn voor bepaalde medewerkers. Stem dit af met directie en de OR. Zorg dat de OR met HR en directie de consequenties van de wijzigingen afstemt en passende maatregelen neemt. Stel in vroeg stadium vast welke medewerkers geschikt zijn voor de nieuwe beheerorganisatie en welke niet.
PR6	Wanneer een ingewikkeld Rule- of Role Based model wordt gekozen, kan dit leiden tot een onduidelijke uitwerking van het model waardoor gebruikersvriendelijkheids-eisen, inzichtelijkheideisen en besparingsdoelstellingen niet worden gehaald. Kies een model welke past bij de organisatie (bijvoorbeeld een organisatorisch, functie gericht of proces gericht model). Dit onderwerp is in de 2e expertbrief verder uitgewerkt
PR7	Wanneer de bedrijfsonderdelen relatief autonoom zijn, is kans aanwezig dat ze uiteenlopende behoefte hebben, omdat ze verschillende uitgangssituaties hebben. Door de uiteenlopende behoefte kan discussie ontstaan over functionaliteit en prioriteit. Voorkom discussies en vertraging door uit te gaan van de businessbenefits voor de organisatie als geheel. Laat dit op directieniveau vaststellen en 'opleggen[3]' aan de bedrijfsonderdelen. Beperk de projectdoelstellingen zoveel mogelijk. Knip daartoe de te behalen beleidsdoelstellingen op over meerdere aaneensluitende (deel-) projecten. Het kan dan zijn dat een divisie voor deze 'eerste' doelstelling meer kosten heeft dan baten. De businessbenefits voor deze divisie kunnen dan in een vervolgproject hoger geprioriteerd worden.
PR8	De wensen van stakeholders lopen in hun formulering vaak zeer uiteen. Het voldoen aan alle wensen is niet mogelijk of blaast het project enorm op. Het is de kunst de wensen van de stakeholders in te vullen door deze te vertalen naar de standaard diensten die geleverd gaan worden. De projectscope en belangen zijn in het architectuurproces (expertbrief 2) al aan de orden geweest. Hanteer die IAM-referentiearchitectuur als uitgangspunt voor de projectopzet. Vermeld dat de projectscope voor de eerste realisatie nog sterk beperkt is en dat een deel van de wensen in een vervolgproject zal worden gerealiseerd. Stem dit duidelijk af en benoem hiervoor duidelijk stakeholders/verantwoordelijkheden.
PR9	Door de complexiteit van het onderwerp en doordat het de gehele organisatie raakt

[3] Opleggen heeft iets autoritairs, het is hier sterk richtinggevend bedoeld, vaak kan de 'pijn' worden verzacht door de decentrale activiteiten centraal te financieren.

	ontstaat er makkelijk ruis op lijn over het project, met alle negatieve gevolgen van dien. Maak van communicatie een deelproject. Dit deelproject richt zich op de in- en externe projectcommunicatie. De interne communicatie betreft o.a. het aanbrengen van een juiste communicatiestructuur tussen de projectleden. Externe communicatie richt zich op de specifieke doelgroepen als: Operationele business: • Afdelingsmanager; • Roleigenaren; • Functioneel beheerders; • Betrokken medewerkers uit de business; • etc.. IT-organisatie: • Technisch en applicatie beheerders; • Fechnisch beheerders; • Servicedesk medewerkers; • etc.. De communicatie naar de operationele business moet zo effectief mogelijk. Het is zaak om hen alleen te informeren wanneer zij er daadwerkelijk iets van merken en hen alleen die informatie te verstrekken die voor hen interessant is. We gaan er hierbij van uit dat er per kwartaal wel iets te melden valt. Als het langer duurt is een tussentijdse nieuwsbrief wel aan te bevelen.
PR10	Het project heeft een relatief lange doorlooptijd. In die periode zal organisatie veranderingen ondergaan die van invloed kunnen zijn op het project. Het kan zijn dat door voortschrijdend inzicht de koers van het project moet worden bijgesteld. Houdt hier rekening mee in de projectopzet. Stel niet te lange termijndoelstellingen en houdt ruimte voor koerswijzigingen. Stem deze tijdig af met de projectboardleden/stuurgroep.
PR11	Soms is (interne) kennis over autorisaties van doelsystemen beperkt aanwezig (met name van legacy-systemen of zelf gemaakte software). Dit kan leiden tot onduidelijke autorisaties in rollen en derhalve tot rolvervuiling. Zorg dat de medewerkers met (oude) kennis van de systemen worden aangehaakt, ook al verrichten zij inmiddels een andere functie.
PR12	Vaak is de initiële functionaliteitwens niet volledig helder. Toolingsfabikanten spiegelen meestal een mooi plaatje voor. Vaak blijkt bij nadere uitwerking en als gevolg van voortschrijdend inzicht dat niet alle functionaliteit wordt geleverd conform verwachting of aanpassingen nodig zijn die extra geld kosten. Stel eerst de interne functionaliteitwensen vast. Bespreek met aansprekende leveranciers de situatie in de vorm van een RFI. Veel leveranciers zijn nog bezig met de ontwikkeling van hun producten, kijk daarom vooral of hun ontwikkelingsroute en –planning aansluit bij de functionaliteitbehoefte van het project en de organisatie op de lange termijn.

PR13	Wanneer gekozen wordt voor een RBAC-oplossing, is de kans dat de hoeveelheid rollen onoverzichtelijk wordt en er daardoor een onwerkbare oplossing wordt geïmplementeerd. Stel van te voren vast welke granulariteit van de rollen nagestreefd wordt. Laat je hierin adviseren door specialisten. Verder uitwerking hiervan staat in de 2e expertbrief.

20

PROJECT PRODUCTEN EN FASERING

Projectproducten en -fasering:
Door aansprekende producten op te leveren en het project te faseren op een wijze die past bij de organisatie kan veel winst worden verkregen. De volgende subvragen zijn dan relevant: Welke producten worden opgeleverd? Welke instrumenten worden gebruikt? Welke hulpmiddelen zijn nodig? In welke volgorde kunnen activiteiten worden uitgevoerd en welke projectfasering past daar bij? Welke aspecten lenen zich het beste als 'quick-wins' op welk moment?

Project producten

Uiteraard dienen enkele producten in lijn te zijn met de intern gehanteerde methoden ten aanzien van projectmethodiek, architectuurmethode, etc.. De hier aangegeven producten zijn genoemd omdat deze volgen uit de eerdere expertbrieven aangevuld met producten die los staan van methodieken.

Nr	Omschrijving
PP1	**Plan van Aanpak** Geef hierin de algemene aanpak aan waarmee de stuurgroep akkoord moet gaan. Dit plan geeft voornamelijk de besturing op hoofdlijnen, de impact, scope en voorziene risico's en business benefits. Denk hierbij aan quick-wins, auditbevindingen et cetera.
PP2	**Requirements document** Deze kan de vorm van een RFI / RFP- Request For Information/ Request For Proposal- krijgen als er tooling geselecteerd moet worden.
PP3	**Communicatieplan (intern/extern project)** Typerend voor AM is de diversiteit van betrokken partijen met eigen belangen en eigen problematiek. Het is daarom van belang vooraf goed na te denken hoe en wanneer deze groepen moeten worden geïnformeerd. Het opstellen van een communicatieplan is daarbij een goed hulpmiddel.
PP4	**Business Case** Zie expertbrief 1
PP5	**Programmaplan** en **(deel)projectplannen** Het programmaplan bevat de beschrijving in hoofdlijnen van alle in de architectuur onderkende plateaus, vertaalt deze naar deelprojecten en voegt de veranderaspecten tot aan het geheel.
PP6	**Governance Charter** In dit charter worden de diverse taken en bevoegdheden vastgelegd.
PP7	**Kwaliteitsplan** Dit document beschrijft de kwaliteitsdoelstellingen, methoden en activiteiten en hangt sterk samen met het requirementsdocument en de wijze waarop het project haar producten ontwikkelt en implementeert.
PP8	**Visie document** Zie expertbrief 1
PP9	**PSA** Zie expertbrief 2

PP10	**Riskmanagement-documenten** Een risicologboek, voorzien van prioriteit en maatregelen.
PP11	**Planning** Bevat zowel centrale als decentrale activiteiten, betrek hierin eventueel ook de planning bij externe leveranciers.
PP12	**AM-Procesbeschrijvingen** Goede beschrijvingen van de AM-processen zijn essentieel voor het slagen van een AM-project. De processen zijn onderdeel van de governance- en beheerinrichting. Procesbeschrijvingen worden hier genoemd als aparte deliverable omdat hier veel van af hangt.

Behoudens deze directe producten zijn er randvoorwaardelijke producten. Soms zijn deze al aanwezig en soms is het AM-project de reden dat deze producten moeten worden gemaakt. Hierbij valt te denken aan:

- Een referentiearchitectuur ten behoeve van meerdere projecten: componenten die je nodig hebt: beleidsstroom, organisatorisch, technisch (OTAP). Verschillende stromen: clustering van componenten. Sommige componenten moeten in samenhang ontwikkeld worden.
- Rolemining tool.
- Role / rule beheertool.
- (Beheer)Documentatie & Procedures.
- Beleid/Policies: Beleid en afgeleide baselines etc. moeten zijn beschreven, anders is het niet mogelijk om te meten of je nu in control bent.
- Maatregelen: policies moeten zijn afgedekt met maatregelen. Wanneer maatregelen uniform zijn, kunnen de oplossingen daarvoor ook uniform zijn. Dat betekent dat deze oplossingen kunnen worden gefaciliteerd door de AM-tooling en dat rapportages over de mate waarin de maatregelen goed worden toegepast centraal beschikbaar zijn.
- Autorisatiematrices.

Role mining wordt door veel vendors aanbevolen als startpunt voor een IAM-traject. Hier is echter een waarschuwing op zijn plaats. Het kan handig zijn om inzicht te verkrijgen in de bestaande situatie. Het doel kan zijn: “aantonen dat de autorisaties dermate complex zijn geworden dat een IAM-traject noodzakelijk is”. Dit is eigenlijk een businesscase motief. Het kan ook worden gebruikt om rollen te modelleren, maar dan alleen als de bestaande situatie al redelijk adequaat is. Role mining checkt namelijk niet waarom de autorisaties zijn verstrekt. Er kunnen dan rollen worden gecreëerd die autorisaties bevatten die om verschillende redenen zijn verstrekt of autorisaties die juist hadden moeten worden ingetrokken.

Bijvoorbeeld: 6 van de 10 medewerkers in een zelfde functie hebben in het verleden ooit meegewerkt aan een project en hebben daarvoor specifieke autorisaties verkregen. Role mining kan aangeven dat deze autorisaties nu in de rol moet worden opgenomen die aan alle medewerkers in deze functie zal worden verstrekt. Echter hadden deze autorisaties juist moeten worden ingetrokken, of in een separate projectrol moeten worden opgenomen. Het gevaar bestaat dus dat er veel tijd verloren gaat in het ontrafelen van een bestaande situatie die eigenlijk helemaal op de schop moet. In zo’n geval is het opzetten van de nieuwe situatie zonder role mining te prefereren.

22

Project fasering

Projecten worden standaard opgedeeld in projectfasen. Voor AM-projecten zijn daarvoor wellicht bepaalde generieke fases te benoemen. Daarvoor gelden de volgende vragen: welke fasering per deelproject is aan te raden en waarom? In welke fase horen welke projectproducten thuis?

De projectfasering moet gericht zijn op het behalen van meetbare resultaten zoals de genoemde plateaus uit de AM-architectuur. Hierbij is het van essentieel belang om ´quick-wins´ te behalen in elk plateau en te groeien in de AM-volwassenheid. Dit kan bijvoorbeeld vorm gegeven worden op de reguliere PRINCE2 fasering.

Het geheel zou er als volgt uit kunnen zien, afhankelijk van wat al aanwezig is kunnen zaken korter of langer duren:

1. Bepaal de architectuur (welk rollenmodel, samenhang, bijvoorbeeld welke rollen zijn gebruikelijk in de branche, soms zijn daar kant en klare rollen voor beschikbaar) Maar ook 1- of 2-laags rollenmodel, de technische architectuur, provisioning strategie (kan gerelateerd worden aan business case). Principes voor het samenstellen van rollen en beheer.
2. Onderscheid een technisch deelproject, een centraal organisatorisch deelproject dat de basis vormt en de decentrale deelprojecten waar de nadruk ligt op de businessrollen.
3. Bepaal de uitrolstrategie, zoals, ga je het doen per bedrijfsketen, dwars door de organisatie heen of pak je alle organisatie onderdelen en ga je afdeling voor afdeling inregelen.
4. Bepaal per bedrijfsonderdeel en/of de te koppelen systemen de uitrolstrategie. Stel aan de hand van de bedrijfsprocessen vast welke rollen nodig zijn, of dat er zelfs nog aanpassingen aan het autorisatiemodel noodzakelijk zijn.

Overigens is de faseringsindeling direct gerelateerd aan de projectdoelstellingen en het beoogde volwassenheidsniveau. Het is in de praktijk erg ambitieus gebleken om vanuit een laag niveau een zeer hoog niveau na te streven. Het is dan beter middels een project een bepaald basis niveau te implementeren en dit niveau langzaam omhoog te krijgen middels het implementeren van een iteratieve verbetermethode (als de Demming-cirkel: Plan, Do, Check, Act) per systeem of aandachtsgebied.

Over het eerste punt ontstond overigens een discussie tussen de werkgroep experts. Sommige vonden dat een AM-project prima van start kan met bijvoorbeeld het doorvoeren van schoningen op de systemen en applicaties zonder over eerst de AM-architectuur na te denken. Anderen vinden wel dat eerst over architectuur moet worden nagedacht, omdat je dan meteen met zo'n schoning een koppeling kan implementeren tussen verstrekte user-id's en een uniek persoonskenmerk als personeelsnummer (zodat ieder user-id te herleiden is naar een medewerker). Voor beide valt wat te zeggen. Het lijkt erop dat het verschil tussen het actuele en nagestreefde volwassenheidsniveau hiervoor een richtlijn is. Worden er ambitieuze doelstellingen nagestreefd, begin dan eerst met architectuur anders wordt veel onnodig/inefficiënt werk verricht. Moeten er kleine stappen worden gemaakt over een langere periode, begin dan alvast met de werkzaamheden die logischer wijs toch moeten gebeuren.

Betrek bij de indeling in fasen de volgende overwegingen:

- Combineer theorie en praktijk. Een te lange ‘studie’-fase haalt het tempo uit het project en resultaten blijven dan uit.
- Zichtbaarheid zorgt voor awareness in alle lagen van de organisatie.
- Laat elke maand voortang/resultaat/succes zien: gebruikers/proceseigenaren zijn meer tevreden.
- Laat snel de basisfunctionaliteit werken. Iedereen ziet dan de businessbenefits van een goed lopend AM-proces. In vele gevallen is de doorlooptijd van het aanvragen van autorisaties aanzienlijk terug gebracht.

24

LESSONS LEARNED PROJECT MANAGEMENT

In bovenstaande hoofdstukken is een aanpak voorgesteld. Dit is een totaal aanpak die op maat gesneden moet worden naar de situatie binnen een bedrijf. In dit hoofdstuk worden enkele handreikingen gedaan om een juiste selectie te kunnen maken. Hiertoe hebben verschillende experts de lessons learned van onderstaande lijst aangedragen.

Lessons learned:

Nr	Omschrijving
LL1	Stel je niet teveel voor van de kwantitatieve businesscase, probeer het een kwalitatieve businesscase te laten zijn.
LL2	Centrale funding en sturing is vereist. Maak niet de fout de deelprojecten decentraal te laten funden.
LL3	Probeer organisatieaspecten uit de roldefinitie te houden. Ervaringscijfers wijzen uit dat procesgerelateerde rollen gemiddeld eens per 3 jaar wijzigen en organisatiegevoelige rollen eens per 2 maanden!
LL4	Probeer de organisatie hiërarchie uit de roldefinitie te houden, grote organisaties hebben vaak een ingewikkelde hiërarchie die niet bijdraagt aan goede roldefinities.
LL5	Essentieel is het laten werken van de basisinfrastructuur met een werkende applicatie waarin basale rollen uitgegeven worden, gekoppeld aan het HR systeem / proces.
LL6	Neem een goede projectarchitect.
LL7	Vermijd namen in ID's, namen wijzigen, gebruik personeelsnummers of beter nog een Authenticatie-ID die gegenereerd wordt uit het personeelsnummers. (Personeelsnummers kunnen wijzigen bij fusies etc.). Houd hierbij rekening met de eisen vanuit de Wet Bescherming Persoonsgegevens (WBP).
LL8	Provisioning kan duur zijn, provision alleen naar toekomstvaste systemen met een hoge mutatiegraad ten aanzien van autorisaties (veel autorisaties/gebruikers).
LL9	Voorzie ook in handmatige provisioning en koppel dat aan het incidentenregistratie systeem. Zo wordt de helpdesk betrokken en raakt men bekend met de materie. De helpdesk kan best hier de bewaking uitvoeren.
LL10	Betrek de business vertegenwoordigers vanaf de start van het project.
LL11	Vergeet de architectuur niet, dat kan je behoeden voor foute keuzes.
LL12	Hoe ga je om met op zich logische rollen, die door systeemtechnische onmogelijkheden niet kunnen worden gerealiseerd.
LL13	Zorg dat je op de hoogte bent van nieuwe releases of vervanging van software, die je planning kunnen verstoren.
LL14	Zorg dat je een goed werkende test-/acceptatieomgeving hebt die een exacte afspiegeling is van de productieomgeving.
LL15	Laat je niet verleiden tot nog even wachten op de nieuwste release van de software, ook die bevat weer nieuwe bugs.
LL16	Zorg dat techniek, organisatie en processen geaccepteerd zijn voor je bedrijfsbreed gaat implementeren.
LL17	Kondig niet te snel aan dat er grote eindproducten aan gaan komen.
LL20	Korte doorlooptijd is belangrijker dan kwaliteit van rollen: Het is beter om niet opgeschoond in productie te gaan dan te wachten tot de laatste eigenaar heeft gereageerd.
LL21	Organiseer een reference site bezoek.
LL22	Steek niet al te veel effort in het vaststellen van de IST situatie. Het met elkaar

	vaststellen van de gewenste situatie en die nastreven is in veel gevallen beter dan een IST situatie vast te stellen die niet als vertrekpunt kan dienen voor verbeteringen.
LL23	Maak een video met de aanvraagprocedure geanimeerd zodat de gebruikers en met name degene die het dagelijks moeten gaan doen (managers of secretaresses) zich in herkennen. Dat is een uitstekend communicatiemiddel en geeft een gezamenlijk doel.
LL24	Het is raadzaam om technische en organisatorische deelprojecten te onderscheiden
LL25	De business aanpak is essentieel, de problematiek die moet worden opgelost speelt een belangrijke rol maar wijk in die zin niet af van de geschetste fasering die ook een voorkeursvolgorde inhoud. Wijk niet af van deze volgorde maar pas de inhoud van deze fasen aan.
LL26	´Quick wins´ blijven altijd belangrijk, zowel voor het halen van doelstellingen als voor de zichtbaarheid van het project. Zorg er dus voor dat spoedig na de start van het project, de ´quick-wins´ behaald worden.
LL27	Een van de belangrijke principes die steeds terugkomen in een autorisatie omgeving is het door de ISO 2700x norm beschreven: “need to know, least privilege” principe. Ondersteund door James Bond achtige films blijkt maar al te vaak dat stukjes op zich niet zo waardevolle informatie bij elkaar toch tot de oplossing van een misdaad kunnen leiden. Helaas is het leven van de doorsnee medewerker in een doorsnee bedrijf, hoe groot ook, niet zo spannend als in een James Bond film….de informatieverwerking is dat ook niet. In een dergelijke omgeving is het niet zinvol om al te restrictief om te gaan met autorisaties. De schade die in een bedrijf ontstaat doordat hier te streng mee wordt omgegaan is vaak vele malen groter dan het schenden van de vertrouwelijkheid van de informatie ooit zou kunnen zijn. Het is dus zaak in een project de BIV-classificatie goed op orde te hebben en stel dit in een vroegtijdig stadium aan de orde zodra je de projectopzet met de medewerkers gaat bespreken. Stel in overleg met de risk management afdeling en de security manager een vragenlijst op en vraag aan de business hoe om moet worden gegaan met dit principe. Bedenk daarbij ook dat autorisatie maar één van de mogelijke maatregelen is die je kunt nemen, denk ook aan application controls en operational controls.
LL28	Een autorisatiestructuur die als het ware logisch past bij de organisatiestructuur wordt al snel geaccepteerd omdat de governance over deze autorisaties goed past bij de bestaande management mandaten. Natuurlijk is dit een ideale situatie die je in de praktijk niet zo vaak zult tegenkomen. Toch is het de moeite waard ernaar te streven.

26

CONCLUSIES EN VERVOLG

De leden van deze expertgroep, zie bijlage 2, hebben antwoorden geformuleerd op de gestelde vragen. Het beoogde resultaat is daarmee gehaald. De ontwikkelingen op dit vakgebied staan echter niet stil, zowel technologisch als qua visie. Deze expertbrief zal derhalve onderhavig zijn aan voortschrijdend inzicht.

De leden van de expertgroep zijn daarom altijd geïnteresseerd in opmerkingen of nieuwe inzichten en nodigen u van harte uit om deze kenbaar te maken. U kunt uw reacties sturen naar expertbrief@pvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen de deelnemers een e-mailtje zeer op prijs!

Hoe verder?
Zoals eerder aangegeven is het onderwerp access management opgesplitst in 4 sessies met ieder een eigen set aan onderwerpen, zie bijlage 1. Ook de resultaten hiervan worden middels expertbrieven verwoord en via de site van het PvIB (www.pvib.nl) beschikbaar gesteld.

Ook via de site www.ibpedia.nl kunt u meewerken aan verdere verrijking en kennisdeling over access management en andere onderwerpen met betrekking tot informatiebeveiliging. Iedereen is van harte uitgenodigd om hieraan deel te nemen.

LITERATUURLIJST

De expertgroep beveelt ter aanvulling of ter verdieping van de behandelde onderwerpen de volgende literatuur aan:

Main bodies:

- Expertbrief “Access management deel1:Visie”, zie https://www.pvib.nl/expertbrief
- Expertbrief “Access management deel2:Architectuur”, zie https://www.pvib.nl/expertbrief
- Expertbrief “security architectuur”, Jaargang 2, nr4, december 2006, zie https://www.pvib.nl/?page=6259972
- Studie Role Based Access Control http://www.pvib.nl
- NIST reeks http://csrc.nist.gov/
- OSA, open security architecture http://www.opensecurityarchitecture.org
- Enterprise Access Management http://www.JPVincent.nl/BIAMEIA
- ISO 27001 & ISO 27002

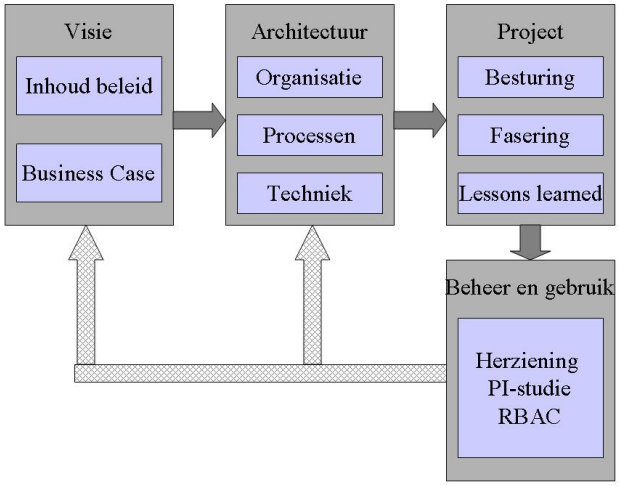
Artikelen:

- Business Oriënted Authorization Model (jaargang 2010,nummer 2) https://www.pvib.nl/kenniscentrum&collectionId=6199206?page=6005940&collectionId=6199206&collections6199206page=2
- RBAC Next generations https://www.pvib.nl/download/?id=6474402&download=1
- ABAC https://www.pvib.nl/download/?id=6474160&download=1
- ABAC https://www.pvib.nl/download/?id=6474183&download=1
- CBAC https://www.pvib.nl/download/?id=10511450&download=1

BIJLAGE 1. SESSIE-OVERZICHT EXPERTBRIEVEN ACCESS MANAGEMENT

Aanpak

De voorbereidingsgroep wil producten opleveren van een hoog kwaliteitsgehalte binnen een reëel tijdsbestek en heeft daarom het onderwerp access management in vier hoofdgebieden opgesplitst (zie figuur 1). Deze hoofdgebieden worden in gescheiden sessies besproken en vallen samen met de stappen die doorlopen moeten worden wanneer men met access management aan de slag wil gaan. Per hoofdonderwerp wordt een expertbrief opgeleverd. Iedere expertbrief kan in principe resulteren in aanvullende themasessies, vervolgartikelen en handreikingen, afhankelijk van de belangstelling en het animo onder deskundigen om hierin te participeren.



Figuur 1.1 Opsplitsing van onderwerp access management in 4 expertbrieven.

De vier hoofdgebieden behelzen het volgende:

1) Visie: Het eerste onderdeel betreft het vormen van een visie over het daadwerkelijk bestaan van één ideaal access management concept. Start een ideaal concept met het hebben van concreet beleid en wat die moet die beschrijven? Het realiseren/implementeren van een compleet access management-concept zal, als gevolg van kosten (businesscase) of complexiteit, niet altijd volledig of in één keer haalbaar zijn. Welke risico's worden onderkent die het succes van een implementatieproject kunnen tegenwerken.

2) Architectuur (deze expertbrief): In het tweede onderdeel wordt access management vanuit architectuur beschreven. Zowel contextueel, als de aspecten omtrent organisatie- en procesinrichting, autorisatiemodellering en techniek.

3) Projectmanagement: In het derde onderdeel zal worden beschreven hoe de implementatie kan worden gerealiseerd en welke werkwijzen en projectinrichtingen daarbij kunnen worden toegepast.

4) Beheer en gebruik: Het vierde onderdeel richt zich op de operationele situatie. Het beantwoord de vraag hoe een beheerorganisatie er concreet uit kan zien, welke ervaringen zijn opgedaan met beschikbare hulpmiddelen, etc. Ook kan, als gevolg de activiteiten van de expertgroepen, de visie op access management zodanig zijn ontwikkeld dat de PI-studie RBAC nader kan worden aangepast.

BIJLAGE 2. INFORMATIE OVER DE DEELNEMERS

Onderstaande deelnemers hebben bijgedragen aan deze expertbrief. Mocht u met een van hen contact willen opnemen dan kan dat via het secretariaat van het PvIB, zie http://www.pvib.nl/contact.

Jean-Pierre Vincent

Vervult rollen als projectmanager, architect en analist in identity & access management-programma's bij grote instellingen in de financiële en telecom branche. Bij zijn werkgever is hij thougt leader identity & access management.

Peter Hoogendoorn

Peter is als security manager betrokken bij een IDM project in de financiële sector en is als consultant, architect en auditor werkzaam geweest in de overheids- en financiële sector.

Karin van de Kerkhof

Karin heeft als consultant ervaring met identity&access management projecten in de overheids- en financiële sector. Is verder werkzaam als auditor.

Danny Mol

Danny is manager Informatiebeveiliging en Security werkzaam in de Public Transport sector en heeft vanuit de invalshoeken beleidsvorming, security management en informatiearchitectuur ervaring opgedaan met Identity en Access Management

Jan-Roel Löwenthal

Jan-Roel is voornamelijk werkzaam in de overheidssector. Houdt zich bezig met Servicemanagement, Architectuur en Informatiebeveiliging. Is bij zijn werkgever focus arealeader van de community identity & access management en heeft op dat vakgebied bij verschillende klanten ervaring opgedaan.

Wiyaykumar Jharap

Wiyaykumar houdt zich als consultant en projectmanager bezig met Security Governance, Risk & Compliance en IAM. Op het gebied van IAM is hij betrokken bij IAM-implementaties in de industriële en semi-overheidssector.

Piet Kalverda

Piet is als security consultant werkzaam in de financiële sector en is betrokken bij de implementatie identity en access management.

Renato Kuiper

Renato is management consultant en richt zich op het snijvlak van informatiebeveiliging, risicomanagement en architectuur. Vanuit die invalshoeken heeft hij veel ervaring opgedaan in Identity en Access Management projecten.

Henk Marsman

Henk heeft meer dan 10 jaar ervaring in informatiebeveiliging. Hij richt zich in zijn huidige rol met name op de onderwerpen Identity & Access Management en Security Management en hoe je deze pragmatisch vorm geeft in een organisatie. Hij heeft zowel auditerende als adviserende rollen uitgevoerd.

Karel van Oort

Karel is als security consultant betrokken geweest bij verscheidene identity en access management projecten.

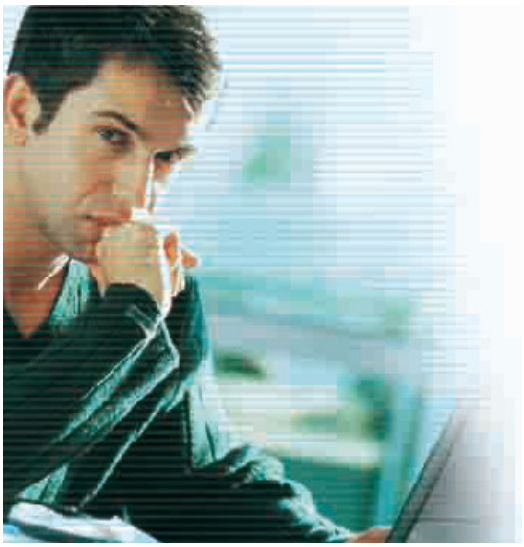
APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by/3.0/nl/

Deze pagina ziet er op het moment van schrijven als volgt uit:

32

WORDT LID VAN HET PVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. Of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Platform voor Informatiebeveiliging kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Platform voor Informatiebeveiliging?
Het PvIB is een open, breed samengesteld platform waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het PvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en IT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

https://www.pvib.nl/abonnementsinformatie