

# Het belang van IT asset management

Drs. ing. P. Olieman

IT asset management is binnen veel organisaties beperkt ingevuld. Uit onderzoek van KPMG blijkt dat organisaties over een beperkt inzicht beschikken omtrent de binnen de organisatie aanwezige IT assets, waardoor tevens het zicht ontbreekt op het eventueel gebruik van illegale software. Twee aandachtspunten zijn hierbij van belang. Ten eerste kunnen organisaties besparingen realiseren door een effectief proces voor IT asset management in te richten, ten tweede vormen softwareaanbieders in toenemende mate een machtsblok om het gebruik van illegale software op te sporen en aan te pakken. Aanbieders leggen boetes op voor illegaal softwaregebruik, waarbij de schade voor een organisatie groter kan zijn dan de boetes alleen.

## Inleiding

Uit een in 2001 breed opgezet onderzoek ([ITAM01]) blijkt dat veel organisaties letterlijk geld verkwisten doordat ze over onvoldoende inzicht beschikken omtrent binnen de organisatie aanwezige IT assets. Organisaties passen als gevolg hiervan bijvoorbeeld meerdere applicaties met sterk overlappende functionaliteit toe. Dit vergt extra beheerspanningen maar bijvoorbeeld ook extra licentiekosten. Een goed opgezet beheer van IT assets kan derhalve aanzienlijke besparingen opleveren, de schattingen lopen uiteen (gebaseerd op bronnen van Meta Group en Gartner) van minimaal tien procent op het totale IT-budget tot dertig procent op de kosten voor het beheren van pc's en servers. Na het uitvoeren van een IT asset audit blijkt regelmatig dat bepaalde software-systemen niet of zeer beperkt worden gebruikt en dus verwijderd kunnen worden.

Door de vele varianten in de licentievoorwaarden is het beheren van licenties vaak complex.

Softwarelicenties dienen adequaat te worden beheerd om te voorkomen dat gebruik wordt gemaakt van illegale software. Wet- en regelgeving (bijvoorbeeld de Auteurswet) en de strijd van bijvoorbeeld de stichting Business Software Alliance (BSA) Nederland tegen 'softwarepiraterij' zijn belangrijke redenen om binnen de bedrijfsmuren illegaal gebruik van software tegen te gaan.

Dit artikel gaat nader in op een aantal statistieken omtrent IT asset management (ITAM) (inclusief illegaal softwaregebruik), de Business Software Alliance ('de softwarepolitie') en de voordelen van een professioneel IT asset managementproces, en geeft een korte weergave van een deel van een methodiek om risico's inzake ITAM binnen organisaties te kunnen vaststellen. Tot slot worden twee praktijkcases beschreven.

## Enkele statistieken

### De mening van de Nederlander

Onderzoeksbureau NIPO heeft in september 1998 een onderzoek uitgevoerd naar de mening van de Nederlander over het gebruik van illegale software ([www.bsa.nl]). Dit onderzoek is uitgevoerd in opdracht van de BSA. In totaal werden 403 vraaggesprekken afgenomen. De respondenten zijn representatief voor de Nederlandse werkende bevolking van vijftien jaar en ouder. Enkele resultaten uit dit onderzoek zijn:

- \* Aan alle respondenten werd de vraag gesteld of zij persoonlijk iets verkeerd vinden aan het kopiëren van computersoftware. Ruim de helft van de Nederlanders (54 procent) beantwoordde deze vraag bevestigend.
- \* Software kopiëren wordt met name gedaan door jongeren, hoogopgeleiden en mannen. Vooral jongeren (tot 39 jaar), degenen die zelf een pc gebruiken of zelf software kopiëren, vinden het kopiëren van computersoftware een minder ernstig misdrijf.
- \* Voor het illegaal gebruik van software voor zakelijke doeleinden is beduidend minder sympathie. Maar liefst 84 procent van de Nederlanders vindt het zakelijk gebruik van illegale software niet geoorloofd.

Met name deze laatste conclusie is van belang; een organisatie die betraapt wordt op het gebruik van illegale software kan namelijk niet alleen een boete tegemoet zien van de softwareleverancier, maar gezien de mening van de ondervraagden is naamschade voor de betreffende organisatie een reëel risico.

### Illegale software en de BSA

De Wet op het Auteursrecht is van toepassing op het gebruik van software. Uit de praktijk blijkt dat een belangrijke reden voor het illegaal gebruik van software gelegen is in het feit dat (te) beperkte IT-budgetten IT-managers in de verleiding brengen om bijvoorbeeld meerdere werkplekken en systemen te voorzien van dezelfde software waarvoor onvoldoende licenties zijn afgenomen. Ook blijkt uit de praktijk dat de betreffende IT-managers vaak wel weten dat ze hiermee licentieovereenkomsten 'ontduiken', maar geen weet hebben van het feit dat hiermee ook relevante wet- en regelgeving niet wordt nageleefd (ze overtreden hiermee de Wet op het Auteursrecht). Een andere belangrijke oorzaak van het aanwezig zijn van onvoldoende licenties ligt in onwetendheid en menselijke fouten. Licentievoorwaarden verschillen van softwareleverancier tot softwareleverancier. Het kan hierdoor voorkomen dat sommige handelingen voor bepaalde leveranciers zijn toegestaan en voor andere leveranciers niet. Door de vele varianten in de licentievoorwaarden is het beheren van de licenties, met name bij grote organisaties, vaak complex. De complexiteit wordt volgens de afnemers van software ook veroorzaakt door het verwarrende licentiebeleid van de softwareleveranciers zelf ([Verk01]).

De BSA is de spreekbuis van meerdere organisaties die software en technologieën ontwikkelen (Adobe, Apple, Autodesk, Compaq, Dell, IBM, Intel, Macromedia, Microsoft, Network Associates, Novell en Symantec). Deze software en technologieën vertegenwoordigen voor de ontwikkelaars in het algemeen een grote waarde en vormen voor hen logischerwijs de bestaansreden. Illegaal kopiëren van software is daarom voor de ontwikkelaars een directe bedreiging voor de continuïteit. De BSA haalt op haar website aan dat het illegaal kopiëren van software binnen organisaties wellicht de belangrijkste vorm van illegaal softwaregebruik is. Volgens dezelfde site wordt in Nederland veertig procent van de zakelijke software illegaal gebruikt (er kunnen geen geldige licenties worden getoond). Nederland behoort hiermee met Griekenland, Portugal, Spanje en Italië tot de top van Europese landen waar illegaal software wordt gebruikt, aldus de BSA. Het Verenigd Koninkrijk doet het volgens de BSA beter in dit opzicht.

**Resultaten recent onderzoek**

In 2001 is in het Verenigd Koninkrijk een onderzoek ([ITAM01]) uitgevoerd om de visie van organisaties te achterhalen met betrekking tot software licensing en hiermee samenhangende procedures. Het onderzoek is uitgevoerd binnen tweehonderd organisaties. Een aantal van de vragen die binnen het onderzoek zijn gesteld alsmede de resultaten worden hierna behandeld.

**Maatregelen om illegaal gebruik van software tegen te gaan**

Op de vraag of de organisatie voldoende maatregelen heeft getroffen om software assets en licenties te kunnen managen, werd geantwoord zoals weergegeven in figuur 1.

65 procent van de respondenten gaf aan dat de eigen organisatie voldoende of meer dan voldoende maatregelen heeft getroffen om illegaal of ongeautoriseerd gebruik van software te kunnen detecteren en tegen te kunnen gaan.

Dit resultaat komt in een ander perspectief te staan wanneer het gekoppeld wordt met een andere bevinding uit hetzelfde onderzoek. Eveneens 65 procent van de respondenten gaf aan dat zij het eens zijn met de stelling dat vele organisaties in het Verenigd Koninkrijk gebruikmaken van software waarvoor geen licenties zijn afgesloten.

**Formeel beleid voor het verwerven van software**

Ongeveer eenderde van de ondervraagde organisaties beschikt niet over een formeel beleid of een formele procedure voor het verwerven van software. Het ontbreken van een formeel beleid verhoogt de risico's voor een organisatie omdat:

- \* de software wellicht kan worden gekocht van een leverancier die geen geautoriseerd verkooppunt is waardoor de software onvoldoende wordt ondersteund door de verkopende partij of door de partij die de software uitgeeft;

- \* de software wellicht niet compatible is met de (toekomstige) infrastructuur van de organisatie (dit risico wordt groter indien een relatie ontbreekt tussen inkoop,

IT-planning, change-management- en configuratiebeheer);

- \* de software bij een verscheidenheid van leveranciers kan worden betrokken waardoor mogelijke schaalvoorwaarden niet worden geëffectueerd.

**Disciplinaire maatregelen**

Hoe de vraag is beantwoord of men het eens of oneens is met de stelling dat tegen werknemers disciplinaire maatregelen moeten worden getroffen indien zij gebruikmaken van illegale software, toont figuur 2.

Uit figuur 2 blijkt dat bijna 97 procent van de respondenten het ermee eens is dat tegen werknemers die gebruikmaken van illegale software, disciplinaire maatregelen dienen te worden getroffen. Uit het onderzoek blijkt verder dat ongeveer eenderde van de ondervraagde organisaties in de praktijk geen formele disciplinaire maatregelen treft indien een werknemer gebruikmaakt van illegale software. Hieruit kan worden geconcludeerd dat organisaties niet over de vereiste procedures beschikken om beleidsrichtlijnen te ondersteunen of dat organisaties in de praktijk de betreffende beleidsrichtlijnen niet bekrachtigen.

**Bewustzijn van risico's omtrent illegaal softwaregebruik**

Op de vraag of de respondenten het eens of oneens zijn met de stelling dat instructies van directie en senior management een positief effect hebben op het verhogen van het bewustzijn omtrent risico's van illegaal softwaregebruik bij personeel en management, werd geantwoord zoals weergegeven in figuur 3.

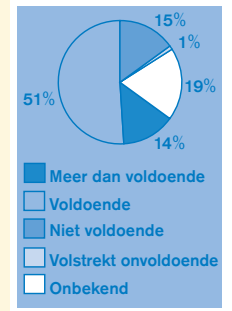
Uit figuur 3 blijkt dat 69 procent van de respondenten het eens is met de stelling. Uit het onderzoek blijkt verder dat slechts weinig bestuurders of directieleden van organisaties de risico's die samenhangen met het gebruik van illegale software, onder de aandacht van de organisatie brengen.

**Een doelgerichte aanpak**

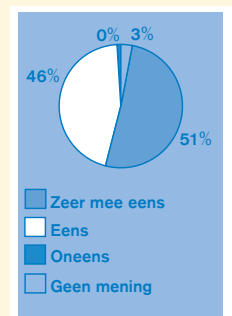
Gezien hetgeen hiervoor is vermeld, is een doelgerichte aanpak van issues aangaande ITAM van belang. Het blijkt dat bepaalde organisaties soms helemaal geen registraties bijhouden van IT assets of soms meerdere registraties bijhouden op papier, met behulp van meerdere toepassingen als MS Excel, MS Access of met behulp van meer professionele geautomatiseerde beheertools. Het gevolg is dat organisaties soms geen inzicht hebben in bijvoorbeeld het aantal in gebruik zijnde installaties van pakketten (en daarmee het benodigde aantal licenties), laat staan of voldaan wordt aan relevante wet- en regelgeving. Een doelgerichte en gestructureerde aanpak van ITAM biedt waarborgen voor het verkrijgen van inzicht in de problematiek en voor het adequaat beheren van de volledige levensloop van IT assets.

**Enkele issues**

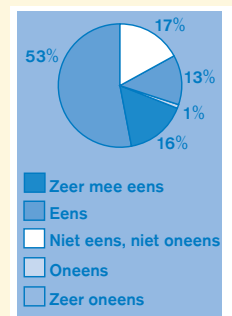
Voor veel organisaties is het niet mogelijk te beschrijven welke IT assets binnen de organisatie aanwezig zijn en of alle software assets voorzien zijn van de vereiste licentie-



*Figuur 1. Management van software assets en licenties.*



*Figuur 2. Het treffen van disciplinaire maatregelen bij illegaal softwaregebruik.*



*Figuur 3. Instructies hebben een positief effect op risicobewustzijn omtrent illegaal softwaregebruik.*



overeenkomsten. Het beeld wordt verder vertroebeld door de wijze van verwerven, installeren, aanpassen en verwijderen van IT assets. In meer detail wordt de vertroebeling veroorzaakt door de volgende omstandigheden:

- \* Een helder aanschafbeleid met betrekking tot IT assets ontbreekt. Zo kunnen er bijvoorbeeld meerdere budgetten beschikbaar zijn voor het aanschaffen van software en hardware en kunnen er meerdere kanalen binnen de organisatie geautoriseerd zijn om IT assets aan te schaffen bij zelf te kiezen leveranciers. Dit leidt al snel tot het ontbreken van een betrouwbaar beeld van de aanwezige IT assets.
- \* Er is geen overall verantwoordelijke voor ITAM.
- \* ITAM heeft een lage prioriteit binnen de directie (totdat partijen als bijvoorbeeld de BSA en individuele softwareproducenten vragen een kijkje in de keuken te mogen nemen).

#### De met ITAM te behalen voordelen

Het invoeren van een ITAM-proces kost natuurlijk tijd, moeite en geld. ITAM houdt namelijk meer in dan alleen het tellen van het aantal in gebruik zijnde pc's en softwarelicenties. Met name het feit dat het invoeren van ITAM geld kost blijkt vaak de reden te zijn waarom organisaties niet beschikken over een geborgd ITAM-proces. Bij het analyseren of het invoeren of professionaliseren van een ITAM-proces voordelen oplevert dienen zowel de mogelijke voordelen die op de korte termijn kunnen worden behaald (de quick wins) als de voordelen die op de langere termijn (tot vijf jaar) kunnen worden behaald, te worden betrokken. Een gefundeerd ITAM-proces heeft over het algemeen de volgende voordelen voor een organisatie:

- \* Alleen die IT assets die strikt noodzakelijk zijn voor de bedrijfsvoering zullen worden aangeschaft.
- \* Het wordt (beter) mogelijk binnen het inkoopproces schaalvoordelen te effectueren.
- \* Het totaal aan administratieve handelingen wordt verminderd (er is slechts één inkoopproces en slechts één registratieproces van IT assets), waardoor de hiermee gemoeide kosten (hoewel vaak verborgen) afnemen.
- \* Specifiek voor software geldt dat het eenvoudiger wordt het aantal licenties in overeenstemming te brengen en te houden met het aantal installaties.
- \* IT-organisaties worden continu geconfronteerd met IT-projecten en derhalve met wijzigingen in de IT-infrastructuur. Het ITAM-proces levert de benodigde managementinformatie om de impact van voorgestelde wijzigingen op de IT-infrastructuur te kunnen vaststellen ([Gart00]). De impact is hierbij breed op te vatten, in termen van kosten en opbrengsten, in termen van activiteiten (vaststellen welke IT assets dienen te worden aan-

gepast of vervangen, vaststellen van de behoefte aan training en tests) en in termen van de benodigde organisatie. IT-projecten worden dus beheersbaarder waardoor een kortere time-to-market van de beoogde projectresultaten wordt gewaarborgd in vergelijking met een concurrent die bijvoorbeeld opereert zonder ITAM-proces.

- \* ITAM is een proces dat overige IT-beheerprocessen ondersteunt waardoor processen als incident & problem management en change management (zie vorige punt) effectiever en efficiënter kunnen worden uitgevoerd.
- \* De kans op virussen neemt af doordat de kans op het gebruik van illegale software wordt verminderd.
- \* Het wordt (beter) mogelijk kosten die samenhangen met het gebruik van IT assets binnen de organisatie effectief door te belasten.
- \* Risico's met betrekking tot het verlopen van onderhoudscontracten en licentieovereenkomsten worden verkleind.

#### Inventariseren van de noodzaak voor professionalisering van ITAM

##### Vier aandachtsgebieden

De ICT-functie binnen een organisatie bestaat uit een vraag- en een aanbodzijde. Figuur 4 bevat de vier aandachtsgebieden die bepalend zijn voor het uiteindelijke resultaat (financieel en kwalitatief) van de ICT-functie: Organisatie, Middelen, Gebruikers, en Processen en applicaties. Ook voor ITAM geldt dat de activiteiten op deze vier gebieden bepalend zijn voor het uiteindelijke resultaat.

Hieronder volgen voorbeelden van aspecten per gebied.

##### ICT-organisatie:

- \* taken en verantwoordelijkheden met betrekking tot licentiebeheer;
- \* kwaliteit van processen en procedures: inkoop van software en hardware, contractbeheer, licentiebeheer, software distributie en -installatie, kostendoorbelasting, verplaatsen en verwijderen van IT assets;
- \* besturing van het ITAM-proces (rapportages);
- \* beleid ten aanzien van budgetten voor aanschaf van IT assets.

##### ICT-middelen:

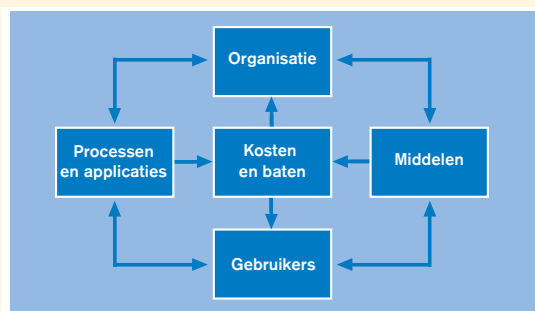
Tools zijn een onmisbaar onderdeel van een effectief IT-assessmentproces ([Trug00]). Er zijn bijvoorbeeld (geïntegreerde) tools voor:

- \* het ondersteunen van het verwervingsproces van IT assets;
- \* het in kaart brengen van aanwezige software assets (zogenaamde tracking of discovery tools);
- \* de vastlegging van de aanwezige IT assets (een configuratiemanagementdatabase);
- \* het meten van het gebruik van software (zogenaamde SUT's, Software Usage Tools);
- \* software distributie.

##### Processen en applicaties:

- \* taken en verantwoordelijkheden van de IT-functie en de gebruikersfunctie met betrekking tot bijvoorbeeld licentiebeheer (afstemmen van vraag op aanbod);
- \* procedures voor het vaststellen van de noodzaak van het gebruik van IT-middelen.

Figuur 4.  
Vier aandachtsgebieden.



*Gebruikers:*

\* kennis en bewustzijn van het belang van licentiebeheer en verwerving van IT assets via de geautoriseerde kanalen.

De auteur hanteert bij onderzoeken naar de kwaliteit van ITAM-processen binnen organisaties als eerste een zogenaamde *health check* waarin onder andere de hiervoor behandelde aspecten aan bod komen. Het doel van de *health check* is snel inzicht te verkrijgen in de toereikendheid van de door een organisatie getroffen (beheersings)maatregelen om de risico's die in dit artikel zijn vermeld, te kunnen voorkomen en beperken. Indien uit het onderzoek blijkt dat de toereikendheid beperkt is, is de noodzaak voor verbetering evident en is tevens meteen duidelijk op welke aspecten (proces)verbeteringen dienen te worden doorgevoerd. Indien van toepassing wordt tevens weergegeven waar mogelijk kostenbesparingen zijn te realiseren. Hierna wordt uitgebreider ingegaan op enkele vragen en onderwerpen uit de *health check*.

*Discovery of IT assets*

Voorbeelden van vragen en aandachtspunten ten aanzien van *discovery of assets* zijn:

- \* Worden er tools ingezet om IT assets in kaart te brengen?
- \* Hoe worden deze tools gebruikt en gehanteerd?
- \* Wordt er een koppeling gelegd tussen het aantal softwaresystemen, het aantal gebruikers en het aantal licenties?
- \* Worden aankoopbewijzen van software adequaat bewaakt?

*Vastleggen van informatie omtrent IT assets*

Het uiteindelijke doel is dat de vastgelegde informatie omtrent de IT assets juist en volledig blijft. Voorbeelden van vragen en aandachtspunten:

- \* In welke mate is het vastleggen van IT assets geïntegreerd met de zogenaamde *discovery tools*?
- \* Welke overige IT-managementprocedures (bijvoorbeeld incident management) hebben toegang tot de vastleggingen en hoe wordt deze informatie gebruikt?
- \* Hoe wordt de juistheid en volledigheid van de vastleggingen gewaarborgd indien het ITAM is uitbesteed aan een derde partij?
- \* Welke details van de IT assets worden vastgelegd?

*Bedrijfsprocessen met betrekking tot ITAM*

Het aanschaffen van IT assets wordt bij voorkeur uitgevoerd door een centrale inkoopfunctie binnen de (IT-) organisatie. Wederom volgen enkele voorbeelden van vragen en aandachtspunten:

- \* Welke formele en informele inkoopkanalen zijn aanwezig?
- \* Hoe verloopt het autorisatieproces met betrekking tot aanschaffen van IT assets?
- \* Hoe complex is het inkoopproces?
- \* Is er een proces geïmplementeerd voor het installeren, distribueren en verwijderen van IT assets en wat is de kwaliteit van dit proces?
- \* Worden fysieke assets gelabeld, en zo ja, hoe?

*Beleid en procedures*

Directie en senior management van organisaties zijn verantwoordelijk voor het juist gebruik van IT assets en voor het voorkomen van illegaal gebruik van software binnen de organisatie. Er dienen daarom beleidsuitgangspunten te worden opgesteld en procedures te worden ingevoerd om te kunnen bewaken dat aan de uitgangspunten wordt voldaan. Voorbeelden van aandachtspunten ten aanzien van beleid en procedures zijn:

- \* eigenaarschap en sponsorschap;
- \* communicatie omtrent beleid en procedures;
- \* het opnemen van uitgangspunten met betrekking tot illegaal softwaregebruik, het downloaden van software en dergelijke in het informatiebeveiligingsbeleid;
- \* disciplinaire maatregelen.

**Do's and don'ts bij software licensing**

Hieronder worden enkele *do's* en *don'ts* met betrekking tot software licensing weergegeven. Ze kunnen worden gebruikt door zowel het senior management als overige medewerkers binnen organisaties en kunnen eventueel in een andere vorm worden opgenomen in bedrijfsinterne beleidsstukken of bewustwordingsprogramma's.

Het senior management dient formeel eigenaarschap te nemen van issues omtrent software licensing.

**Do's**

- \* Het senior management binnen de organisatie dient formeel eigenaarschap te nemen van issues omtrent software licensing.
- \* Stel een standaard samen voor noodzakelijke softwaresystemen die op iedere desktop (laptop) en server moeten worden geïnstalleerd. De standaard dient tevens te worden gedocumenteerd in het IT-beleid en in het informatiebeveiligingsbeleid.
- \* Stel een heldere strategie vast met betrekking tot het toepassen van software welke geen onderdeel vormt van de standaard-softwareportfolio.
- \* Stel een heldere procedure op voor het aanschaffen (op welke wijze dan ook: huren, leasen, kopen) van software.
- \* Tracht het aantal softwareleveranciers te minimaliseren zodat inkoopvoordelen kunnen worden bereikt.
- \* Maak gebruik van betrouwbare softwareleveranciers.
- \* Bepaal en bekrachtig procedures voor het aanschaffen van software en hardware. Deze procedures dienen het volgende te bevatten: bestellen, leveren, installeren, wijzigen, verplaatsen, verwijderen, upgraden, het actualiseren van de configuratiemanagementdatabase en het bewaren van documentatie waaruit eigenaarschap en/of het recht op gebruik van de middelen blijkt. Tevens dient in de procedures aandacht te worden besteed aan het reconciliëren van de documentatie betreffende eigenaarschap / recht op gebruik en de daadwerkelijke software geïnstalleerd op desktops/laptops en servers.



*Drs. ing. P. Olieman* is werkzaam als manager binnen KPMG Information Risk Management, waar hij in 1996 in dienst is getreden. Zijn specialisaties zijn IT-audits en adviesopdrachten op het gebied van risicobeheersing binnen IT-projecten, IT-beheer en (out)sourcing.

- \* Stel een helder beleid op met betrekking tot het gebruik van niet-zakelijke software en communiceer dit beleid binnen de organisatie.
- \* Stel een informatiebeveiligingsbeleid op en neem hierin beleidsuitgangspunten op (of neem deze op in het bestaande informatiebeveiligingsbeleid) met betrekking tot niet-gelicenseerde (illegale) software, inclusief disciplinaire maatregelen indien medewerkers toch van dergelijke software gebruikmaken.
- \* Het senior management dient daadwerkelijk disciplinaire maatregelen te treffen indien één of meer medewerkers gebruikmaken van ongeautoriseerde (niet passend bij de standaard-softwareportfolio) en illegale software.
- \* Maak gebruik van een configuratiemanagementdatabase en implementeer procedures en tools die de actualiteit en volledigheid van deze database kunnen waarborgen.
- \* Voer regelmatig (bij voorkeur onaangekondigd) compliance audits uit met betrekking tot de procedures.
- \* Waarborg dat alle betrokkenen kennisnemen van de procedures en beleidsuitgangspunten met betrekking tot issues inzake software licensing en van het belang van het naleven van deze procedures voor zowel de organisatie als de medewerkers zelf.

#### Don'ts

- \* Sta niet oogluikend toe dat illegale software wordt gebruikt.
- \* Sta niet toe dat software wordt gedownload (de kans bestaat dat de software illegaal is, bovendien kunnen er virussen worden geïntroduceerd).

#### Praktijkcases

##### Een telecom provider in het Verenigd Koninkrijk

Het management van een telecom provider was er redelijk van overtuigd dat voor alle software die op de servers was geïnstalleerd, licenties waren afgesloten en dat alleen van zakelijke software gebruik werd gemaakt. Men wilde echter aanvullende zekerheid verkrijgen omdat de BSA een bezoek had aangekondigd. Uit onderzoek naar de daadwerkelijk geïnstalleerde software bleek al snel dat de overtuiging van het management niet volkomen terecht was. Er bleek een ruime hoeveelheid spellen te zijn geïnstalleerd (waaronder enkele pornografische), alsmede een significante hoeveelheid software die niet was geregistreerd binnen de beschikbare software-inventaris.

Een verdere analyse binnen de organisatie maakte duidelijk dat naast de spellen ook een deel van de overige niet-geregistreerde software niet voor noodzakelijke organisatiedoelinden werd gebruikt. Deze software werd verwijderd, waardoor de benodigde tijd werd geminimaliseerd voor het controleren van de overige software met als doel te bepalen of die software van de nodige licenties was voorzien. Verder bleek dat ook een deel van deze software nooit werd gebruikt. Deze soft-

ware werd geback-up't en verwijderd van de server; geen van de 'gebruikers' heeft hierover achteraf geklaagd. Met de leveranciers van deze software werd contact opgenomen om de lopende licentieovereenkomsten alsmede de onderhoudscontracten te beëindigen. Het bleek bij deze organisatie niet nodig aanvullende licentieovereenkomsten te sluiten.

#### Financiële instelling in Nederland

Door diverse interne ontwikkelingen diende een financiële instelling de automatiseringsorganisatie te professionaliseren. Teneinde de diverse IT-beheerprocessen zoals incident management, change management en problem management goed te kunnen inrichten, was een eenduidige vastlegging van de software assets van essentieel belang. Om permanent over een actueel en volledig overzicht van de software assets te kunnen beschikken was het inrichten dan wel verder professionaliseren van ITAM noodzakelijk.

De eerste stap was het uitvoeren van een assessment naar de betrouwbaarheid van de softwareregistraties. Allereerst zijn alle aanwezige softwareregistraties in kaart gebracht, dit waren er drie in totaal, te weten een registratie in MS Excel, een in Lotus Notes en een registratie in een helpdesktool. Geen van de registraties bleek compleet noch juist. Om een volledig en juist overzicht te krijgen zijn naast het matchen van de registraties tevens interviews gehouden met medewerkers van de afdeling Informatiesystemen binnen deze organisatie.

Het resultaat was een betrouwbaar overzicht van de aanwezige software. Analoog aan de vorige casebeschrijving bleek een significant deel van de software niet langer nodig te zijn en kon het aantal lopende licentieovereenkomsten en onderhoudscontracten worden beperkt. Het behoeft geen betoog dat de mogelijke besparingen groot waren.

#### Literatuur

- [Gart00]  
*IT Asset Management: The quest to be smart and rich*, Gartner, 3 February 2000.
- [Hunt01]  
B. Hunt, *IT mismanagement costs businesses 17 bn Pounds a year*, Financial Times, 27 September 2001.
- [ITAM01]  
KPMG, *The 2001 KPMG IS/IT Asset Management Survey*, June 2001.
- [Trug00]  
M. Truglio-Kirwin and P. Adams, *IT Asset Management tools: discover the difference*, Gartner Research Note, 9 May 2000.
- [Verk01]  
P. Verkooijen, *Agressie BSA blijft controversieel*, ITIQ, VNU Business Publications, december 2001.
- [www.bsa.nl]  
<http://www.bsa.org/nederland/globalib/nipo.phtml>