Opzet van wereldwijde sofware compliance audits bij Philips

Nan Zevenhek

Steeds meer organisaties worden zich bewust van de noodzaak tot software compliance en vooral van het belang van een goede bewijsvoering. In contracten van softwareleveranciers staat vaak dat deze audits mogen uitvoeren om te controleren of bedrijven voldoen aan de bepalingen van hun softwarelicenties. Philips heeft afgelopen jaren een aanpak ontwikkeld om de risico's met betrekking tot software compliance te kunnen beoordelen en verminderen.

Auteur

Drs. N. (Nan) Zevenhek RE is sinds 1 januari 2008 verantwoordelijk voor Global IT Asset Management bij Philips. In haar vorige functie bij Internal Audit heeft ze software compliance audits opgezet.
Ze heeft ervaring in internationale logistieke en financiële systemen. Zevenhek is eveneens fractievoorzitter van het CDA te Waalre – zie www.cdawaalre.nl – en lid van het Algemeen Bestuur van Waterschap de Dommel.

Bedrijven zijn wettelijk verplicht om voor software die geïnstalleerd is op hun computers de eventuele licenties te betalen of een ander soort vergoeding te voldoen. De laatste jaren vragen steeds meer softwareleveranciers om zogenaamde software compliance audits, om zekerheid te krijgen over de volledigheid van dergelijke betalingen. Philips vindt het ongewenst dat leveranciers dat zelf intern uitvoeren, omdat er dan heel veel Philips locaties zijn die met externe partijen hierover moeten communiceren.
Tegelijkertijd zijn bedrijven zich bewust van de kosten van software en willen niet meer licentiekosten betalen dan strikt noodzakelijk. In beide gevallen spelen er financiële aspecten: qua boetes en qua bedrijfsvoering. Bij het niet-compliant zijn is er ook het risico van imagoschade.
Tijdens een conferentie in maart 2007 in Utrecht over IT Asset Management werd duidelijk dat veel bedrijven geen zekerheid kunnen geven over het compliant zijn met de bepalingen van hun softwarelicenties[1].
Sinds vier jaar voert *Philips Corporate Internal Audit* jaarlijks interne software compliance audits uit. De scope wordt vastgesteld door het *Philips Audit Committee IT* met als voorzitter de *Chief Financial Officer*. Deze audits staan in principe los van verzoeken van externe leveranciers, maar houden er wel rekening mee.
Dit artikel beschrijft 'meetaspecten' van de bewijsvoering, softwarelicenties bij Philips en de wereldwijde opzet van software compliance audits bij Philips en ervaringen daarmee.

Meten van software en licentieadministratie

Bij veel softwarepakketten is bij de ontwikkeling geen rekening gehouden met de wijze waarop het aantal installaties of het gebruik ervan gemeten kan worden. Ook de licenties zelf hanteren verschillende gebruikscriteria. Daardoor zijn er heel veel variaties in de wijze van meten van software en de administratie van licenties.

Voorbeelden van meting van het gebruik van geïnstalleerde software op de machines zijn:

- Agents, die automatisch tijdens het inloggen van een gebruiker een scan maken van welke software geïnstalleerd is op de computer, of scans die regelmatig draaien op computers die verbonden zijn aan het lokale netwerk.
- Handmatige metingen, waarbij alleen een geautoriseerde persoon in staat is software te installeren en er regelmatig

een onafhankelijke steekproef genomen wordt van wat daadwerkelijk geïnstalleerd is. Dit is alleen werkbaar bij kleine organisaties.
- Een leveranciersspecifieke oplossing die apart meten overbodig maakt, zoals een licentiesleutel, waarmee een beperkt aantal installaties mogelijk is. Of een ingebouwde logfile, die het aantal gebruikers bijhoudt en die niet aangepast kan worden. Het maximum aantal gebruikers dat gemeten is, moet dan bijvoorbeeld betaald worden.

Speciale aandacht is nodig voor computers die op voorraad liggen met daarop geïnstalleerd software. Afhankelijk van de contractvoorwaarden moet die wel of niet meegeteld worden in de metingen.

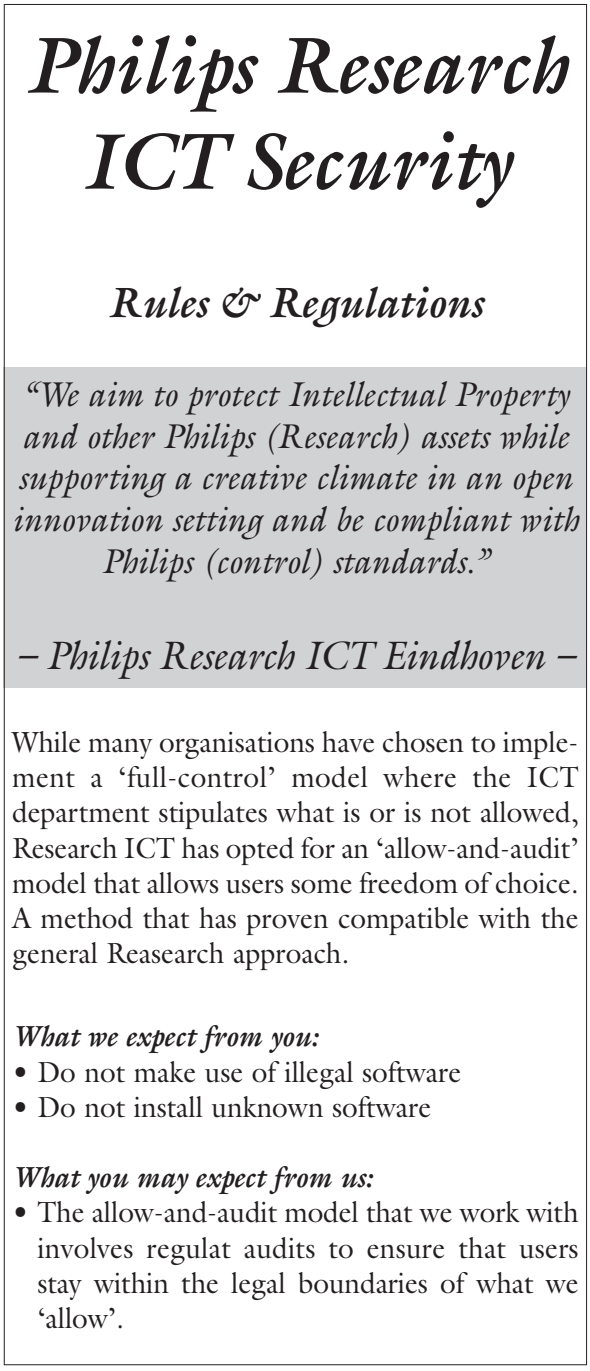
Voorbeelden van administratie van beschikbare softwarelicenties zijn:
- Excel sheets, waarop handmatig de ingekochte licenties worden vermeld, met de geldigheidstermijn en andere gegevens.
- Databases die vanuit bijvoorbeeld een SAP-systeem gegevens krijgen van aangekochte softwarelicenties en automatisch of handmatig gevuld worden met informatie van een systeem dat geïnstalleerde software scant.
- Configuration Management Database systemen die handmatig worden bijgehouden.

Softwarelicenties bij Philips

Phlips heeft wereldwijd 121.700 mensen in dienst, verspreid over 26 landen. Bij de aanvang van 2007 waren er vier verschillende Product Divisies.
Omdat er geen standaards waren hebben IT-managers van Philips zelf een methode ontwikkeld die voorziet in de mogelijkheid om het aantal beschikbare licenties ten opzichte van het aantal geïnstalleerde licenties te meten en daarover te rapporteren.

Bij wie of welke functie ligt de verantwoordelijkheid voor software compliance?
Softwarelicenties worden beschouwd als een asset. De verantwoordelijkheid voor de asset en de software compliance ligt altijd bij de business die gebruik maakt van de software. Afhankelijk van het soort software, kan de verantwoordelijkheid gedelegeerd zijn.
Voor een aantal grote contracten (bijvoorbeeld SAP, Oracle en IBM) is *General Purchasing IT* verantwoordelijk en onderhoudt het primaire contact met een leverancier. De licenties worden centraal voor Philips ingekocht en kunnen via een zogenaamde License Desk gefactureerd worden aan bedrijfsonderdelen. Voor andere centrale contracten worden lokaal inkooporders bij het afgesproken verkoopkanaal geplaatst.
Voor standaard kantoorsoftware is er een centrale uitvoerende IT-organisatie, die handelt namens de business. Deze zorgt ervoor dat een aantal softwarepakketten vooraf betaald zijn (bijvoorbeeld Windows XP Professional) en zorgt tevens voor distributie van (updates van) de software. De business rapporteert hoeveel *Qualified Desktops* ze van een pakket geïnstalleerd heeft en betaalt daarvoor maandelijks een bedrag.

De wijze waarop bedrijfsonderdelen intern hun software compliance regelen is sterk afhankelijk van de eisen en karakteristieken van de business. In fabrieksomgevingen of bedrijfsonderdelen met een lage winstmarge zijn er strikte regels voor de aankoop van software. Als een business daarentegen hoge winstmarges heeft, wordt er minder gelet op mogelijke kosten, maar wordt er bijvoorbeeld wel sterk gelet



Figuur 1: 'Allow and audit statement' bij research

op beveiliging. Bij researchafdelingen moeten onderzoekers juist de vrijheid hebben om het nieuwste van het nieuwste uit te proberen, waaronder softwarepakketten. Behalve een potentieel licentieprobleem is er ook een beveiligingsrisico, omdat onbekende en ongeteste software ongewenste effecten kan hebben. Hier zijn harde (ondertekende) afspraken met gebruikers nodig en wordt een zogenoemd 'Allow and audit' model toegepast. Gebruikers mogen zelf software installeren, maar dienen de IT-afdeling hiervan op de hoogte te brengen, zodat die de software kan onderzoeken. Men dient zelf te regelen dat er voldoende licenties zijn aangekocht. Regelmatig voert de IT-afdeling audits uit op de naleving van deze afspraak.

Auditen van software compliance bij Philips

Internal Audit van Philips maakt gebruik van een zogenaamde 'risk based approach'. Daarbij gebruikt ze een inschatting van de risico's voor de opzet van haar audits.

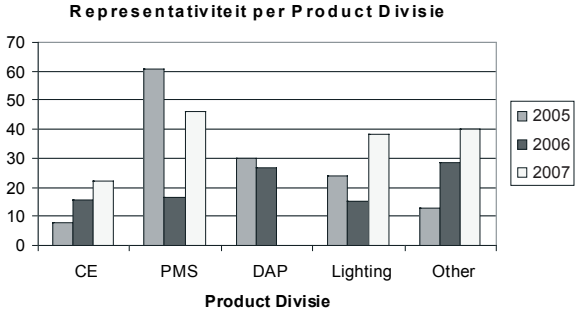
Voor software compliance zijn de volgende algemene risico's gedefinieerd:

- ontbreken van voldoende kennis op het gebied van softwarelicenties.
- illegale software is geïnstalleerd, met gerelateerde beveiligingsrisico's of ongeplande interactie met reguliere software.
- onjuiste of onvolledige administratie van het aantal geïnstalleerde softwarepakketten.
- onjuiste of onvolledige administratie van aantal beschikbare softwarelicenties.
- teveel en te dure software is geïnstalleerd.

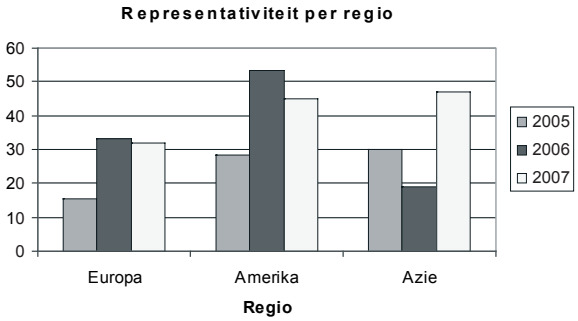
Het laatste risico kan ook geformuleerd worden als 'ontbreken van kostenbewustzijn'. Adobe Acrobat Professional is bijvoorbeeld veel duurder dan Adobe Acrobat Elements. De meeste gebruikers maken alleen een PDF-file aan, waarbij Elements al voldoende is.
Het financiële risico is afhankelijk van het softwarepakket, hoe de inkoop van de licenties verloopt – centraal of decentraal – en hoe de fysieke distributie van software plaatsvindt.

Voor de grote centraal beheerde softwarepakketten worden Philips-breed gegevens opgevraagd en vergeleken met het aantal licenties. Afhankelijk van de details van het licentiecontract moeten gegevens tussen bedrijfsonderdelen afgestemd worden, om te voorkomen dat gebruikers dubbel meetellen. Internal Audit zorgt hierbij voor ondersteuning en een controleerbare opzet van de metingen en wijze van rapporteren. Bijvoorbeeld voor SAP heeft Internal Audit meegeholpen met een draaiboek voor het uniform meten van de SAP installaties per Product Divisie en het definiëren van de te meten grootheden, zodat de verzamelde gegevens vergelijkbaar waren. De wijze van ondersteuning of auditen is geheel afhankelijk van het soort pakket, de contracten en de achtergronden van de vraag.
Dit artikel gaat daar niet verder op in, maar gezien de grote juridische en financiële risico's heeft software compliance van deze pakketten veel aandacht binnen Philips.

Bij software waar men lokaal verantwoordelijk voor is, heeft Internal Audit een opzet gemaakt voor de compliance audit. De aanpak is afgelopen vier jaar sterk verbeterd. Er worden wereldwijd locaties geselecteerd en fysiek bezocht.
In eerste instantie was er een willekeurige selectie van locaties, waarbij één auditor de hele wereld rond reisde. Pas in het tweede jaar werd achteraf gekeken hoe representatief de geselecteerde locaties waren ten opzichte van het geheel en naar de verdeling over de Product Divisies en de regio's.



Figuur 2: Representativiteit van geaudite locaties per Product Divisie



Figuur 3: Representativiteit van geaudite locaties per regio

In 2006 werd al bij de selectie van locaties gekeken of de verdeling over de continenten en Product Divisies evenredig was. De toen onderzochte locaties waren verantwoordelijk voor beheer van 22,5 procent van het totale aantal 'Qualified Desktops' binnen Philips. Door de inspanningen voor SOx waren er beduidend minder locaties bezocht.
Omdat het reizen toch relatief veel tijd kostte, is in 2007 een andere strategie voor de selectie van locaties gekozen. Bij al geplande operationele audits is nagegaan of gelegenheid was een software compliance audit uit te voeren en of er totaal voldoende verdeling was over de regio's en Product Divisies. Deze aanpak was weer efficiënter omdat er geen tijd (en geld) aan reizen verloren ging. Er was echter meer coördinatiewerk nodig, om de compliance audits toe te voegen aan reeds geplande audits.

In 2008 zal de software compliance audit onderdeel worden van de reguliere Performance Reviews. Daarbij worden vele aspecten van de bedrijfsvoering geaudit. De representativiteit van de daarbij geselecteerde bedrijfsonderdelen ten opzichte van het totaal aantal PC's is nog onbekend.

Jaartal	2004	2005	2006	2007
Aantal uitvoerende auditors	1	9	4	11
Aantal onderzochte locaties	19	32	20	30
Totaal benodige uren per locatie inclusief voorbereiding en reizen	23	13	10	10
Wijze van selectie locaties	random	random	dekkings-graad	operationele audits
Representativiteit geaudite locaties t.o.v. total aantal PCs	?	30%	20%	35%

Tabel 1: Karakteristieken van software compliance audits bij Philips

Bij grote tekortkomingen vindt een jaar later altijd weer een software compliance audit plaats, soms door een nieuw lokaal bezoek, maar ook door een telefonisch interview en opvragen van digitale bewijzen.

Auditvoorbereiding, veldwerk en rapportage

Bij de wereldwijde software compliance audits van de desktops en laptops is een coördinerend Audit Manager verantwoordelijk voor de administratieve voorbereiding, planning, ondersteuning en eindrapportage.
Alle *Chief Information Officers* van de Product Divisies krijgen een algemene *Engagement Letter* met een aankondiging van de onderwerpen en de opzet van de audit, zonder de geselecteerde locaties zelf te noemen.
De lokaal verantwoordelijk auditor, stuurt uiterlijk drie dagen voor het fysieke bezoek een aankondiging. Dit kan omdat het auditveldwerk zelf bij goede voorbereiding maar een paar uur in beslag neemt.
Per locatie is er een *template file* beschikbaar, waarin per risico kan worden aangegeven welke maatregelen zijn genomen om het risico te beperken. De toelichtende informatie is zodanig dat er bijna geen uitleg nodig is.

Bij de voorbereiding beoordeelt de Audit Manager de ontwikkelingen in de centraal gerapporteerde cijfers van het aantal Qualified Desktops en de geïnstalleerde standaardsoftware. Hij formuleert daarbij vragen die de lokale auditor kan stellen, naast de algemene vragen.

- Het is bijvoorbeeld zeer onwaarschijnlijk dat er drie kwartalen achtereen hetzelfde aantal gerapporteerd wordt: aantallen computers en softwarepakketten in een organisatie zijn vrijwel altijd aan verandering onderhevig.
- Een grote variatie in de tijd is echter ook onwaarschijnlijk en vereist een goede (organisatorische) uitleg.
- Om het kostenbewustzijn te beoordelen wordt gekeken naar de verhouding tussen het aantal dure pakketten en het aantal goedkope pakketten met ongeveer dezelfde functionaliteit.

Tijdens het veldwerk legt de lokale auditor de antwoorden op de vragen in de template vast. Bij tekortkomingen, bijvoorbeeld te weinig of te veel licenties, wordt de ernst van de tekortkoming ('rating') bepaald op basis van het bedrag dat er mee gemoeid is. De software compliance wordt beoordeeld als inadequaat als:

- Uit de beantwoording van de vragen blijkt dat er lokaal geen kennis aanwezig is over softwarelicenties en er geen duidelijke procedure is voor installeren en deïnstalleren van software en beheer van aangekochte licenties.
- Als er geen automatische scan is van geïnstalleerde software en aantoonbaar compenserende maatregelen ontbreken. Het aantal bevoegde personen voor Admin rechten op een PC of Laptop moet bijvoorbeeld beperkt zijn en regelmatig moet handmatig de geïnstalleerde software vergeleken worden met de administratie. Anders wordt de werkwijze beschouwd als een groot risico en belangrijke tekortkoming.
- Als het gerapporteerde aantal niet overeenkomt met het gescande aantal en er geen reële verklaring is voor de afwijking.

Als bewijs vraagt de auditor om ter plekke een aantal systeemscans te verrichten en/of beoordeelt hij/zij de gebruikte systeemscan. Voor vooraf centraal geselecteerde softwarepakketten vraagt de auditor kopieën van de facturen voor de betreffende software. Bij *concurrent* softwarelicenties controleert de auditor in het systeem of daar het maximum aantal overeenkomt met datgene wat in de licentie staat.

De auditor maakt zo snel mogelijk een samenvatting van zijn bevindingen en legt de verzamelde bewijzen digitaal vast. Dit kan ook in de vorm van screenprints. Na overeenstemming met de auditee over de bevindingen, kan de locatie direct met eventuele verbeteracties beginnen. Bij grote tekortkomingen worden hogere managementniveaus en de Financial Controller geïnformeerd.
In november/december maakt de coördinerende Audit Manager een formeel rapport per Product Divisie. Algemene bevindingen worden onderscheiden van bevindingen per Product Divisie of per regio. Om de kennisuitwisseling te verbeteren, verwijzen bijlagen van het rapport naar Best Practices of internationale ontwikkelingen.

Effecten

Er gaat een preventieve werking uit van software compliance audits: Product Divisies gebruiken bijvoorbeeld de Engagement Letter om bij hun lokale IT-personeel het belang van

software asset management extra te benadrukken. Informatie uit de rapporten wordt gebruikt voor distributie van kennis.
De software compliance en vooral het bijhouden van de licentiepositie door bedrijfsonderdelen van Philips is sterk verbeterd.
Het algemene bewustzijn van het belang van Software Asset Management is sterk vergroot. Ook op hogere niveaus in de organisatie beseft men dat software een asset is, waarbij goed beheer zichzelf terug verdient.
Centrale afdelingen nemen een deel van de audit taak over, omdat op basis van de administratieve analyse van gerapporteerde cijfers vaak al te voorspellen is of een locatie adequaat softwarelicentiemanagement heeft of niet. Een regionale IT manager kan een bedrijfsonderdeel daardoor preventief adviseren en ondersteunen.
Door de systematische opzet van de audits is redelijk in te schatten hoeveel tijd nodig is voor het coördinerende werk en het veldwerk lokaal.

Verbetering van de onderhandelingspositie

Door kennis van de eisen van de business kunnen onderhandelingen met leveranciers doelmatiger gevoerd worden. Daarbij gaat het niet alleen over de prijs, maar ook of er specifiek gemeten moet worden en wat de meeteenheid is.
Een bedrijfsonderdeel van Philips heeft bijvoorbeeld bereikt dat ze een 'named user' licentie mocht vervangen door een 'concurrent users' licentie. Voor de leverancier had dit als voordelen een vergroot draagvlak voor betaling van een weinig gebruikt pakket en een sterk vereenvoudigde controle.
Ook omzetting van een licentie van serverniveau naar een hoger niveau (meestal een fysieke locatie met meerdere bedrijfsonderdelen), kan een interessante optie zijn. *K-SOL Project Reader* staat het bijvoorbeeld toe dat er op een locatie ongelimiteerd gebruik van dit pakket kan worden gemaakt, zonder het actuele aantal installaties of gebruik te hoeven meten.

Conclusies

Een systematische aanpak van software compliance audits loont. De afgelopen jaren is bij Philips het software asset management sterk verbeterd en kan audit zich specifiek richten op regio's of bedrijfsonderdelen waar risico's liggen of op grotere softwarepakketten.
Bij software waar bedrijfsonderdelen zelf volledig verantwoordelijk voor zijn, kunnen lokale auditors heel goed de compliance beoordelen. Voorwaarde is dat er een compacte, maar heldere instructie is met achtergrond, vragen, mogelijke antwoorden en voorbeelden van bewijsvoering.
Voor de grote centraal beheerde pakketten lijkt een vast aanspreekpunt voor uitvoering van software compliance audits essentieel. Bijvoorbeeld voor tussentijdse advisering. Daarbij is een specialisatie in Software Asset Management van de auditor onvermijdelijk gezien de complexiteit van de bewijsvoering en betrokkenheid van verschillende disciplines.
Naar aanleiding van de bevindingen ontwikkelt Philips een 'sense and simplicity' proces, dat zorgt voor beperking van de juridische en financiële risico's en de mogelijke imagoschade. ■

Aanbevelingen

Het bijhouden van Master data zoals 'fingerprints' of 'DNA' waaraan software herkend kan worden, kost veel tijd. Er is een ISO-norm in ontwikkeling voor het definiëren van deze zogenaamde Tags[2].
Herkenbaarheid van software is ook in het belang van de leverancier. Bedrijven kunnen de onduidelijkheid gebruiken als oorzaak dat het bewijzen van software compliance bemoeilijkt wordt, of een andere leverancier selecteren die het wel goed geregeld heeft.
Er is afgelopen jaren een ISO-norm voor Software Asset Management ontwikkeld[3], waar sommige bedrijfsonderdelen al gebruik van maken. Met deze ISO-norm kan ook het auditen zelf weer verbeterd worden, of zich richten op andere terreinen van Software Asset Management die voorwaardenscheppend zijn.
Te eenvoudige installatie van software, zonder aan te geven welke keuzes met de daaraan gerelateerde kosten mogelijk zijn, kan leiden tot dure en veel te geavanceerde softwarepakketten. Door het aantal keuzes te beperken en te stimuleren (en regelmatig te controleren) dat er vooral standaardsoftware wordt gebruikt, kan dit voorkomen worden.
Belangrijk is dat de meeteenheid van een softwarelicentie of contract eenduidig vastligt. Als dit onduidelijk is, kan de organisatie hierop onvoldoende sturen en kunnen onverwachte financiële verplichtingen het gevolg zijn.
Veel softwarelicenties blijven ongebruikt, die mogelijk op andere plaatsen in het bedrijf ingezet kunnen worden. Informatie hierover is vaak onvoldoende bekend of bereikt niet de juiste personen.
Een lokale 'License Advisory Board' en een speciale softwarelicentiemanager kunnen veel geld besparen: bedrijfsonderdelen die hun licentiepositie goed beheersen en zich bewust waren van de kosten, concentreerden zich op het efficiënter gebruik van de softwarelicenties, door ongebruikte software te deïnstalleren en goedkopere pakketten aan te bieden. Ook ging men in onderhandeling met leveranciers. Er zijn bedrijfsonderdelen waarbij de complianceverplichting met een paar miljoen euro verminderd is. Voor totaal Philips is het bedrag onbekend.

Noten

1 Conferentie IT Asset Management 21 maart 2007, Heliview, Utrecht
2 De laatste ontwikkelingen staan op http://www.iso19770.com
3 ISO/IEC 19770-1 over Software Asset Management, zie http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33908&ICS1=35&ICS2=80&ICS3=&scopelist