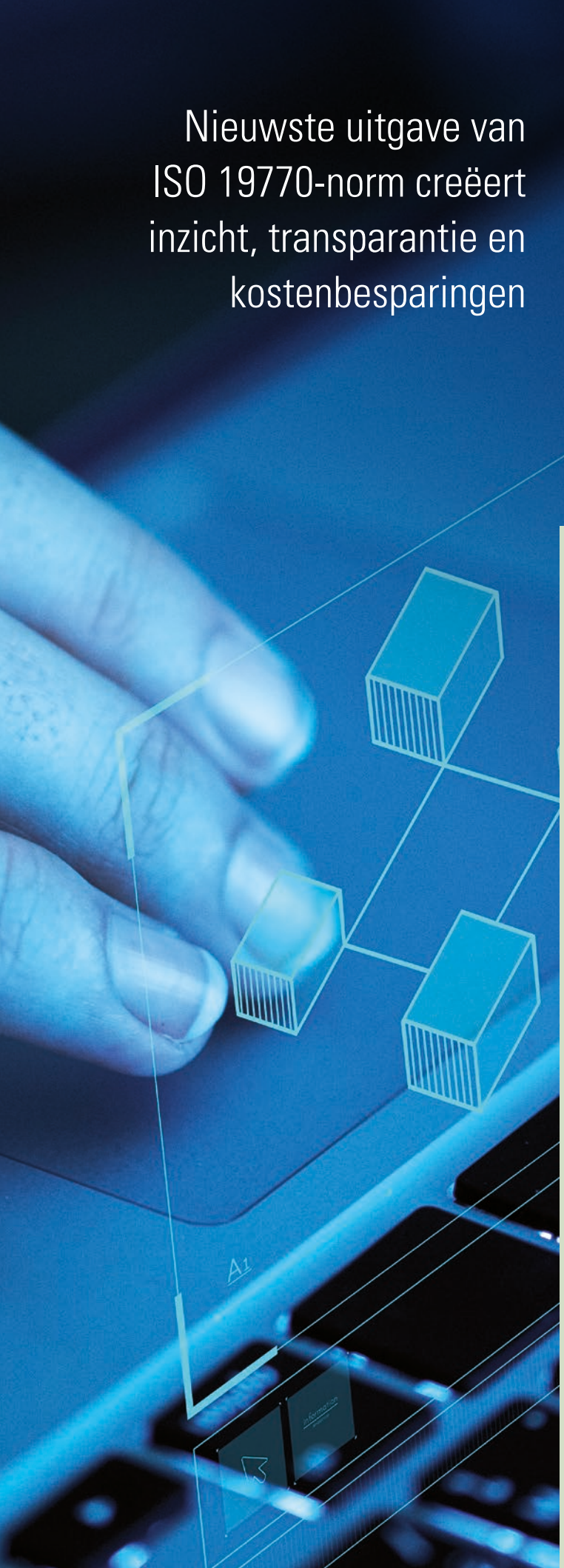
Nieuwste uitgave van ISO 19770-norm creëert inzicht, transparantie en kostenbesparingen

Software Asset Management



Een belangrijke voorwaarde om vertrouwen te hebben in een IT-omgeving zijn gedocumenteerde processen rondom softwaregebruik, inclusief bijbehorende licentievoorwaarden. Software Asset Management (SAM) stelt organisaties in staat om op een slimme en effectieve wijze hun softwarerechten te beheren, vanaf het moment van aanschaf tot aan de vervanging ervan. De nieuwste editie van de ISO-norm, ISO/IEC 19770:2017, biedt organisaties handvatten om de gekozen doelstellingen van SAM te realiseren. In dit artikel wordt naast de facetten van de ISO-norm ook ingegaan op de voordelen van SAM, en op welke wijze dit geïntegreerd kan worden binnen een organisatie.

Wouter Pluim LLB
is werkzaam in de Software Asset Management-praktijk van KPMG.
pluim.wouter@kpmg.nl

Leon Huijsman MSc RE CISA
is werkzaam als Software Asset Management -analist bij CRH.
leon_huijsman@hotmail.com

INLEIDING

'SAP claimt 600 miljoen dollar van AB Inbev', 'Mars daagt Oracle voor de rechter' en 'Nike en Quest verwikkeld in juridisch gevecht': koppen in de media die allemaal te maken hebben met het gebruik van software en de interpretatie van licentieovereenkomsten.

Op vrijwel alle software rust een intellectueel eigendomsrecht. Applicaties moeten worden ontwikkeld en aangepast aan nieuwe technologieën en continu wijzigende wensen van de afnemers. Softwareleveranciers die softwarepakketten ontwikkelen en verkopen, beogen hun gemaakte investeringen via de exploitatie van de software terug te verdienen. Dit kan door uiteenlopende voorwaarden op te stellen voor de gebruikers van de programmatuur. Door middel van een licentie wordt het gebruiksrecht verschaft, waarin beperkingen kunnen worden gesteld aan het gebruik van de software in bijvoorbeeld een bepaalde gebruiksomgeving, het aantal apparaten, geautoriseerde gebruikers of de rekenkracht van de server. Complexe meeteenheden kunnen voor organisaties desastreuse gevolgen hebben, wanneer de kennis en kunde om deze software op de juiste wijze in te zetten ontbreekt. Meer dan eens ontstaan er problemen met software die op gevirtualiseerd niveau is ingekocht, en vervolgens op fysiek niveau wordt geïnstalleerd.

Softwareleveranciers nemen in hun overeenkomsten vaak clausules op die hen het recht geven om licentieaudits uit te voeren bij hun klanten. Tijdens een dergelijke audit wordt in kaart gebracht of de aangeschafte licenties overeenkomen met de software die daadwerkelijk is geïnstalleerd, of op andere wijze beschikbaar is gesteld aan de gebruikers. Na het vaststellen van de licentiepositie volgen geregeld discussies tussen de klant en leverancier om de geconstateerde licentietekorten op te lossen. Als uitkomst hiervan worden vaak – door gebrek aan inzicht, juridische druk of angst voor boetes – extra softwarelicenties aangeschaft. Meer dan eens betreft dit licenties voor geïnstalleerde software die de organisatie bij nader inzien helemaal niet nodig blijkt te hebben. Zo kan software per abuis worden geïnstalleerd, per ongeluk worden verwijderd, of op onjuiste wijze worden ontsloten, waardoor meer gebruikers toegang hebben dan de bedoeling was (en waarop werd ingekocht). Het kan aanzienlijke negatieve, financiële consequenties voor een organisatie hebben wanneer deze tekorten worden geconstateerd tijdens een licentieaudit. Naast de financiele risico's zijn er diverse andere risico's die het gebruik van software en beheer van licenties met zich meebrengt; denk hierbij aan beveiligingsrisico's, reputatieschade en slecht functionerende software. Zo kan onbeheerde software beveiligingsrisico's met zich meebrengen. Wanneer het installeren van updates en patches niet op geautomatiseerde wijze plaatsvindt, kan onbeheerde software verouderen, en daarmee een potentieel beveiligingsrisico voor de organisatie vormen. Denk hierbij aan de wereldwijde WannaCry-aanval. Bovendien kunnen security-incidenten en/of negatieve uitkomsten van licentieaudits resulteren in aanzienlijke reputatieschade voor een organisatie. Dergelijke problemen zijn schadelijk voor het vertrouwen van een organisatie in de IT-omgeving. Software Asset Management (hierna SAM) is ontwikkeld om aan deze operationele, financiële en compliance-risico's tegemoet te komen.

De IT Infrastructure Library (ITIL) ([Rudd09]) omschrijft SAM als alle infrastructuur en processen die noodzakelijk zijn voor het effectief managen, controleren en beschermen van softwarebezittingen binnen een organisatie. Oftewel: het totale proces rondom het beheer

Aanvullende controls nodig bij verwerking software assets in asset management-systeem

Om de nieuwste versie overzichtelijker en makkelijker te kunnen integreren, is in de versie van ISO 19770 uit 2017 aansluiting gezocht met ISO 55001 over Asset Management. In ISO 55001 zijn standaarden bepaald ten aanzien van het opzetten, implementeren, onderhouden en verbeteren van een managementsysteem voor asset management. ISO 19770 (hierna ISO) bevat ten opzichte van 55001 aanvullende eisen, daar waar het gebruik van software specifieke eisen met zich meebrengt, die bij het 'traditionele' asset management niet van toepassing zijn. Deze norm omvat onder andere eisen met betrekking tot:

- controls ten aanzien van softwaredistributie, -duplicatie en -modificatie, met de nadruk op toegankelijkheid en integriteitsmaatregelen;
- het creëren van audit trails ten aanzien van toegekende autorisaties en aanpassingen die gemaakt worden aan IT-assets;
- controls ten aanzien van licensing, onder- en overlicensing, en compliancy ten aanzien van licentievoorwaarden;
- controls ten aanzien van situaties waarin sprake is van 'mixed ownership' en verantwoordelijkheden, zoals bij cloud computing of BYOD-toepassingen;
- de reconciliatie en integratie van IT-asset management data van bijvoorbeeld financiële systemen ([ISO17-2]).

en de optimalisatie van de planning, inkoop, implementatie, onderhoud en uitfasering van software assets binnen een organisatie. SAM kan bijdragen aan het ontwikkelen van effectieve processen en waarborgt de continuïteit van de IT-omgeving, waarmee uiteindelijk het vertrouwen in IT wordt vergroot.

In dit artikel wordt, naast een algemene inleiding over Software Asset Management en het toepassingsgebied, ingegaan op de nieuwste ISO-norm: ISO/IEC 19770:2017. Verder worden de volwassenheidsniveaus van organisaties ten aanzien van SAM (uitgedrukt in Tiers binnen ISO 19770) behandeld. Tot slot wordt inzicht gegeven in de integratie met andere bedrijfsprocessen.

De scope van SAM omvat elk type software en de gerelateerde assets

SOFTWARE ASSET MANAGEMENT

ISO 19770-ontwikkeling

ISO 19770:2017 is ontwikkeld om organisaties concrete handvatten te bieden om 'in control' te zijn ten aanzien van software assets. Het betreft inmiddels de derde grote uitgave van norm 19770 binnen twaalf jaar. De eerste versie uit 2006 beschreef SAM-processen en bevatte harde standaarden om controle uit te oefenen ten aanzien van software assets. In 2012 werden hier enkele nuances in aangebracht, en werd onderscheid gemaakt tussen vier verschillende volwassenheidsniveaus van SAM, ook wel aangeduid als Tiers. Deze Tiers waren respectievelijk 'Trustworthy Data', 'Practical Management', 'Operational Integration' en 'Full ISO/IEC SAM Conformance'. Het ambitieniveau van deze laatste en hoogste Tier is achteraf bezien wellicht wat onrealistisch gebleken, aangezien voor zover bekend geen enkele organisatie dit niveau heeft weten te bereiken. Mede daarom is in 2017 het aantal Tiers teruggebracht van vier naar drie. Organisaties worden weliswaar handvatten geboden, maar het is aan de organisatie zelf om te bepalen welke activiteiten van belang zijn om haar doelstellingen te bereiken. De drie Tiers zullen later in dit artikel uitvoeriger aan bod komen.

De scope van SAM omvat uiteindelijk elk type software en de gerelateerde assets, ongeacht wat voor type software het betreft en op welke wijze het aan de gebruikers ter beschikking wordt gesteld. Zo kan het bijvoorbeeld gaan om uitvoerende software (zoals een operating system), niet-uitvoerende software (een woordenboek, verschillende lettertypen in een programma, et cetera) of software die niet na een installatie gebruikt wordt, maar bijvoorbeeld op connectie gebaseerd is, of software as a service. Hierbij kan gedacht worden aan het gebruik van software via smartphones, cloud-based software of hosted software.

In veel organisaties is door de jaren heen een wildgroei aan applicaties ontstaan, waarbij gebruikers zelf over rechten beschikken om software te installeren. De oplossing hiervoor is een organisatie-breed uitgerold SAM-beleid, waarbij software centraal beschikbaar wordt gesteld aan gebruikers, en er niets lokaal geïnstalleerd kan worden. Dit is echter niet mogelijk bij BYOD, waar gebruikers uiteraard wel zelf software kunnen installeren. Organisaties kunnen hieraan tegemoetkomen door een beleid te hanteren waarbij duidelijk is wie verantwoordelijk is voor de software op het betreffende apparaat.

Het toepassingsgebied van SAM voor wat betreft het type organisatie varieert bovendien ook. Zo kan een SAM-programma binnen multinationals of in kleinere (MKB)-organisaties worden opgezet, gecentraliseerd of gedecentraliseerd worden opgezet, of worden geoutsourcet ([ISO17-1]).

Voordelen en doelstellingen van SAM

In ISO wordt onderscheid gemaakt tussen twee categorieën voordelen die met SAM gerealiseerd kunnen worden om de bovengenoemde risico's te mitigeren. Dit zijn enerzijds voordelen op het gebied van kostenbeheersing, anderzijds de realisatie van een hoger niveau van risicomanagement ([ISO17-1]).

Kostenbeheersing
Een asset is iets wat mogelijk of daadwerkelijk waarde heeft voor een organisatie ([ISO14]). Deze waarde kan zowel positief als negatief zijn, afhankelijk van de fase van de levenscyclus waarin de asset verkeert.

Naast de waarde van een (IT-)asset, en daarmee dus ook een software asset, kent de aanschaf van licentierechten in veel gevallen een hoog kostenplaatje. Aan de hand van een verrichte enquête concludeert Spiceworks ([SPIC18])

dat doorgaans 26 procent van het totale IT-budget wordt besteed aan de aanschaf en het jaarlijks terugkerend onderhoud van software. In 2017 gaf Gartner ([GART17]) hiervoor een bandbreedte aan van 18 tot 26 procent. Hoewel het daadwerkelijke percentage per organisatie zal verschillen, kan wel worden gesteld dat de kosten aanzienlijk zijn.

Het beheersen van deze kosten, en daarmee de waarde van een asset vergroten, is een van de belangrijkste doelstellingen die is opgenomen in ISO. Op diverse procesgebieden van SAM kunnen kosten worden bespaard. Bij het onderhandelen over contracten met softwareleveranciers kunnen betere prijzen gerealiseerd worden, wanneer er een scherp beeld bestaat van de behoefte van de organisatie, en welke huidige contracten er afgesloten zijn. Een voorwaarde is wel dat de organisatie beschikt over betrouwbare data, zoals hiervoor beschreven. Niet zelden komt het voor dat organisaties licenties aanschaffen waar ze via een reeds afgesloten contract al recht op hebben. Ook zullen de onderhandelingen met leveranciers minder tijdrovend zijn, als er een duidelijk beeld van de huidige licentiepositie (en behoefte) vanuit de organisatie wordt geschetst. Bovendien kan er zo accurater gebudgetteerd en begroot worden.

Kwalitatief hoogwaardige SAM-processen brengen bovendien met zich mee dat software op efficiëntere wijze wordt ontsloten aan de gebruikers en software beschikbaar wordt gesteld op basis van behoefte, en niet omdat het kan. De beheerskosten en licentie-uitgaven worden hiermee beperkt. Ten slotte stellen monitoring tools de organisaties in staat om nog niet-geïdentificeerde softwarecomponenten te identificeren ([ISO17-1]).

Iedere organisatie dient zelf af te wegen welke risico's acceptabel zijn

Het managen van verschillende soorten risico's

Naast de wens, of soms zelfs noodzaak, van directe kostenbeheersing is er bij het gebruik van IT-assets altijd sprake van risico's. Deze risico's zijn verschillend van aard, bijvoorbeeld:

- operationeel (disruptie van IT-beschikbaarheid of verminderde kwaliteit hiervan);
- security (autorisatiemechanismen, herkenning van niet-geautoriseerde software en het ontwikkelen van een update- en patchproces);
- non-compliance (licentie non-compliance, reputatieschade, persoonsgegevens en bijbehorende privacy-risico's).

De risicocategorieën kennen wel een gemene deler. Niet of verkeerd gemanagede risico's kunnen leiden tot financiële schade. Dit kan resulteren in directe schade in de vorm van boetes of onnodige extra uitgaven, maar ook in indirecte schade in de vorm van gemiste inkomsten door reputatieschade. Met het implementeren van SAM-processen kunnen deze risico's deels worden geminimaliseerd.

Het implementeren van alle beschreven operationele processen is, ook volgens ISO, niet voor elke organisatie een realistische optie. Er zal dan ook een weloverwogen keuze voor een acceptabel geacht risiconiveau moeten worden gemaakt. Zo kent bijvoorbeeld kostbare software – met een licentie per processor core in een gevirtualiseerde omgeving – een hoger risico op non-compliance dan een fysiek werkstation, waarop goedkope software is geïnstalleerd die per installatie een licentie vereist. In dit geval helpt SAM om deze software en de waarde ervan in kaart te brengen, op basis waarvan vervolgens een risico-inschatting kan worden gemaakt. Het maken van zo'n risico-inschatting is een onderdeel van het risicomanagement.

ISO schrijft voor dat, op basis van een risico-inventarisatie, verschillende plannen en processen geformuleerd moeten worden om:

1. risico's en kansen ten aanzien van IT-assets te identificeren;
2. veranderingen ten aanzien van eerdere geïdentificeerde risico's tijdig op te merken;
3. criteria vast te stellen waarop risico's beoordeeld worden;
4. criteria vast te stellen voor welk risico acceptabel is;
5. eigenaren van risico's aan te wijzen;
6. prioriteiten te stellen voor welke risico's eerder behandeld moeten worden.

Iedere organisatie dient zelf af te wegen welke risico's acceptabel zijn. Voor IT-assets is gedegen onderzoek naar de mogelijke risico's geen overbodige luxe. Dit geldt in het

bijzonder voor software assets. Het creëren van processen voor het beheer van softwareassets, die ook gemonitord en bijgehouden moeten worden, kan door de veelheid aan producten een onmogelijke opgave worden. Aan de hand van verschillende criteria kan een selectie worden gemaakt van de software assets met de hoogste prioriteit.

Gezien de continue dynamiek van IT-landschappen is het identificeren van risico's en het bijhouden van de veranderingen ten opzichte van reeds bekende risico's onontbeerlijk. De bewustwording ([ISO17-2]) van eventuele risico's aangaande IT-assets bij alle betrokkenen binnen een organisatie wordt steeds belangrijker. In het verleden was een IT-organisatie redelijk goed in staat om het gebruik van IT-assets te beperken of af te schermen. Technologische ontwikkelingen stellen gebruikers echter in staat om steeds meer zelf te doen op het gebied van IT. Dit uit zich onder meer via BYOD en bijvoorbeeld cloud-oplossingen, die rechtstreeks door de gebruiker worden afgenomen en gevuld met data. Deze nieuwe vormen van IT maken het identificeren van risico's een stuk complexer.

Kortom, het prioriteren van risico's binnen een organisatie is sterk afhankelijk van de mate waarin deze bepaalde risico's acceptabel acht.

IT ASSET MANAGEMENT TIERS

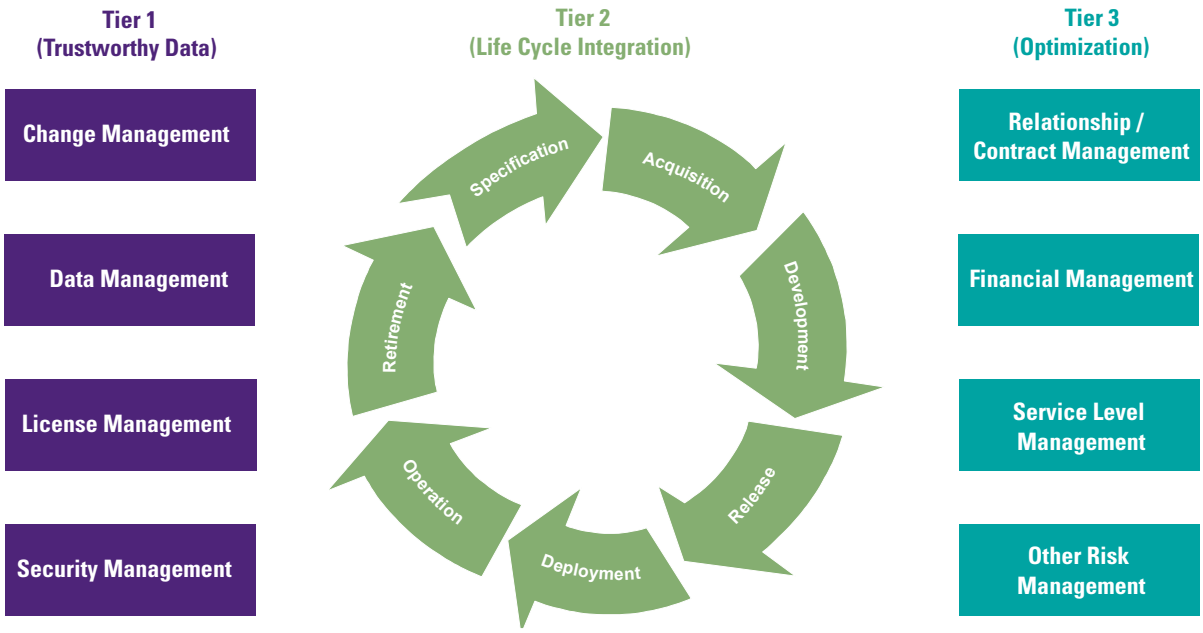
De processen ten aanzien van het management van IT assets worden gegroepeerd in Tiers, waarmee het volwassenheidsniveau van het door de organisatie geïmplementeerde SAM en de IT asset managementprocessen wordt aangegeven. De Tiers zijn ontwikkeld om tegemoet te komen aan de behoefte van de markt. Het bleek voor veel, met name kleinere organisaties namelijk niet realistisch (of zelfs onmogelijk) om alle processen volledig te implementeren. Tegelijkertijd bleef de behoefte aan zekerheid en licentie-compliance wel bestaan. Dit heeft geleid tot de volgende cumulatieve categorisering, die bijdraagt aan het vertrouwen van een juiste inzet van IT(-assets):

Tier 1: Betrouwbare data
Het bereiken van deze Tier houdt in dat een organisatie 'weet wat het heeft', en zodoende besluiten kan nemen op basis van adequate informatie. Een organisatie beschikt in deze Tier over redelijke zekerheid ten aanzien van compliance.

Tier 2: Lifecycle-integratie
Met het bereiken van deze Tier wordt meer efficiency gerealiseerd en worden kostenbesparende maatregelen met betrekking tot de IT-software-lifecycle getroffen.

Tier 3: Optimalisatie
In de derde Tier wordt nog meer efficiency en effectiviteit gerealiseerd, door de nadruk te leggen op diverse functionele managementgebieden, zoals relatie- en contractmanagement, financieel management en servicelevel-management).

Figuur 1. SAM Tiers en procesgebieden – detailbeschrijvingen van de onderdelen van elke Tier zijn terug te vinden in het kader.



Het is aan de organisatie zelf om het ambitieniveau ten aanzien van SAM te bepalen

SAM IN UW ORGANISATIE

Een organisatie met een SAM-functie, waarin aandacht wordt besteed aan de beschreven procesgebieden, zal raakvlakken hebben en geïntegreerd zijn met uiteenlopende processen en/of afdelingen binnen een organisatie, die zijn weergegeven in Figuur 2. Hierin wordt schematisch weergegeven welke activiteiten en afdelingen betrokken kunnen zijn bij Tier 1 of 2, en ten slotte bij een optimale inrichting van het SAM, zoals beschreven is in Tier 3. Duidelijk wordt dat de verwevenheid van het SAM met de organisatie toeneemt naarmate een hogere Tier wordt gerealiseerd.

De inkoopafdeling is in deze organisatie verantwoordelijk voor het inventariseren van de behoefte aan software en het contact met de diverse softwareleveranciers. Het betrekken van de afdeling Inkoop is een voorwaarde voor het hebben van betrouwbare data, en daarmee een typisch 'Tier 1-proces'. Dit geldt ook voor de juridische afdeling, die bij een contractonderhandeling erop toeziet dat er geen verplichtingen worden aangegaan die strijdig zijn met de (interne) compliance.

HR-informatie wordt gebruikt als actuele informatiebron voor de hoeveelheid gebruikers en het ter beschikking stellen van richtlijnen ten aanzien van softwaregebruik binnen de organisatie. Bovendien is het user-lifecycle-management via HR geregeld, en vindt derhalve ook het beschikbaar stellen van de software aan de medewerkers plaats. Wanneer een medewerker weer uit dienst gaat, of een andere functie krijgt, dienen zijn of haar toegewezen licenties weer ingetrokken te worden, zodat deze kunnen worden hergebruikt. Een dergelijke integratie van het SAM met andere bedrijfsprocessen is een voorbeeld van een doelstelling in Tier 2.

Procesgebieden van functioneel management van IT-assets (waaronder software assets)

De Tiers van SAM zijn gebaseerd op verschillende functionele IT-asset-procesgebieden. Zoals te zien is in Figuur 1 zijn deze gekoppeld aan de eerste en derde Tier ([ISO17-2]). Per Tier zullen hieronder de elementen worden toegelicht.

Tier 1: Trustworthy Data

Change management
Dit betreft het gecontroleerd plannen van veranderingen, inclusief het rekening houden met en reageren op onverwachte wijzigingen (en het beperken van onbedoelde gevolgen daarvan).

Datamanagement
Proces om ervoor zorg te dragen dat alle IT-assets gedurende de gehele lifecycle op een juiste wijze zijn geregistreerd en geverifieerd. Dit proces is een cruciale voorwaarde voor het hebben van betrouwbare data, en vormt hiermee een noodzakelijk uitgangspunt voor de effectiviteit van andere bedrijfsprocessen. Het verifiëren van data is hierbij een essentieel onderdeel om aan de voorwaarde van betrouwbaarheid te kunnen voldoen.

Licentiemanagement
Dit omvat het proces om een accurate licentiepositie te bewerkstelligen, oftewel: waar heeft de organisatie recht op, en wat is er in gebruik? Binnen dit proces worden periodiek reconciliaties uitgevoerd tussen het actuele gebruik en de beschikbare licenties. Afhankelijk van de gekozen scope van licentiemanagement kunnen rechten aangaande digitale content ook onder licentiemanagement vallen.

Securitymanagement
Proces voor effectieve en gecontroleerde beveiligingsmaatregelen voor IT-assets. Deze maatregelen omvatten toegangs- en integriteitscontrole van de assets in scope en assets die informatie bevatten over IT-assets. Wanneer de doelstellingen van de bovenstaande vier procesgebieden gerealiseerd worden, is voldaan aan de eerste Tier.

Het managen van de processen in de levenscyclus van IT-assets

Binnen Tier 2 ligt de focus primair op de softwarelevenscyclus (zie Figuur 1) en de doelstellingen binnen deze processen.

Tier 2: Lifecycle Integration Specificatie
Het proces voor het inventariseren van de behoefte binnen een organisatie en het beoordelen van mogelijke alternatieve scenario's in relatie tot de aanschaf van IT-assets.

Acquisitie
Proces dat erop toeziet dat de aanschaf van IT-assets op gecontroleerde wijze plaatsvindt en op deugdelijke wijze wordt vastgelegd.

Ontwikkeling
Specifiek gericht op het hebben van een proces op het gebied van software-ontwikkeling en het voldoen aan de eisen die voortvloeien uit IT-asset management.

Ontsluiting / operationele inzet
Proces dat erop toeziet dat het vrijgeven van IT-assets volgens planning en op correcte (geautoriseerde) wijze wordt uitgevoerd.

Uitrol
Proces dat op het inzetten van IT-assets toeziet en tevens hergebruik mogelijk maakt.

Beheer
Proces voor het juist gebruiken van IT-assets. Dit omvat onder andere het monitoren, optimaliseren en verbeteren van de prestaties van de IT-assets. De reeds aangehaalde functionele managementprocessen dienen te integreren met dit proces. Denk bijvoorbeeld aan licentiemanagement, waarmee de operationele inzet van software geoptimaliseerd wordt. Daarnaast vallen de huishoudelijke taken als back-up en opschoning onder beheer.

Inname en herbestemming
Proces voor het verwijderen van IT-assets, inclusief eventueel hergebruik in overeenstemming met dataretentie/-vernietiging-verplichtingen.

Verdieping en optimalisatie van de procesgebieden van functioneel management van IT-assets

Tier 3: Optimization
Nadat de doelstellingen van Tier 2 zijn gerealiseerd (zie hierboven) kan een organisatie besluiten de voordelen van SAM ten volle te benutten, en zich richten op de laatste Tier. Tier 3 bestaat uit de volgende procesgebieden:

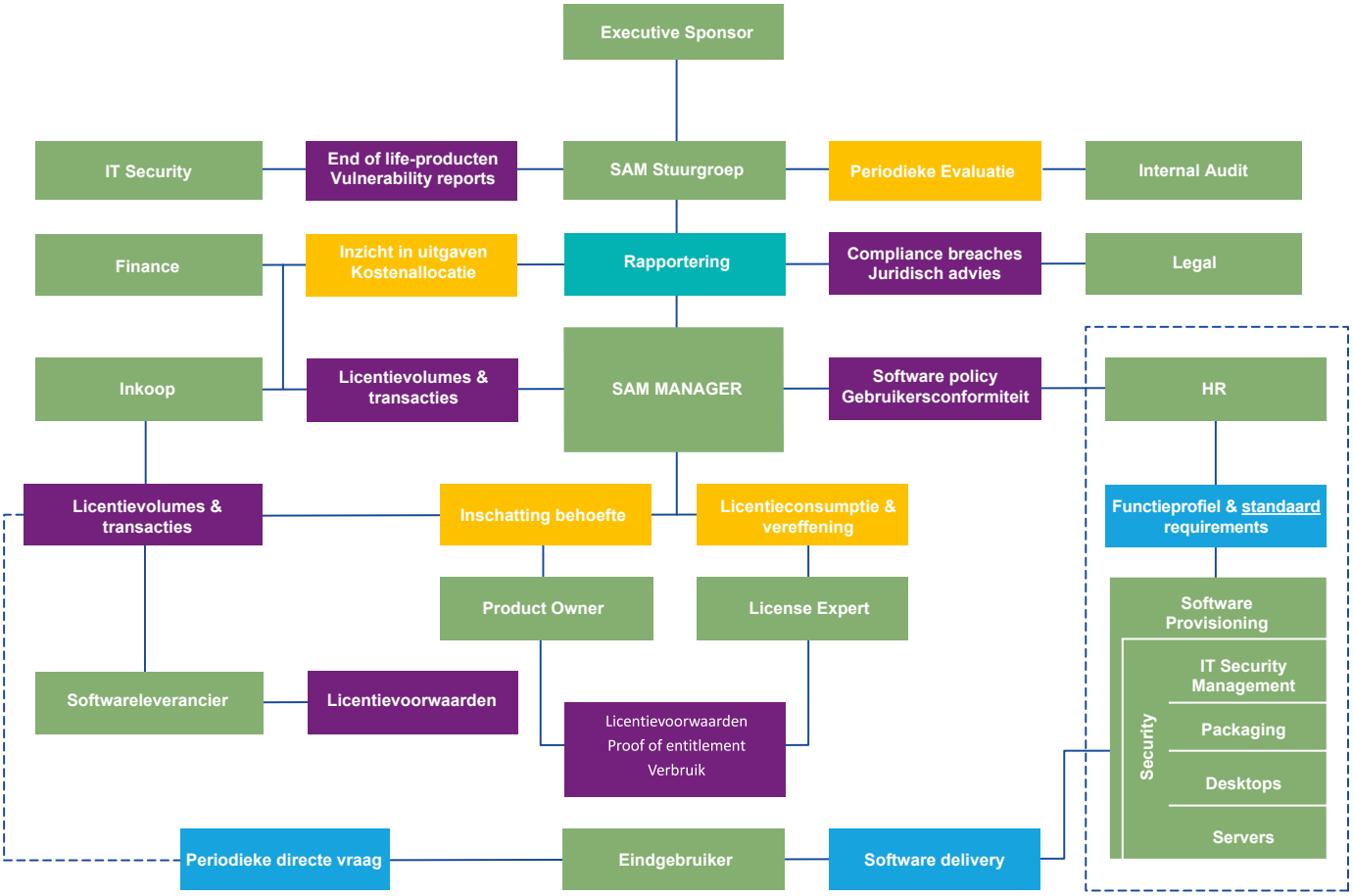
Relatie- en contractmanagement
Het effectief managen van de interne en externe relaties aangaande IT-assets. Dit is inclusief de verificatie van het naleven van contractuele verplichtingen, bovenop de verplichting van licentiemanagement.

Financieel management
Proces om de kosten en waarde van IT-assets te monitoren en beheren, inclusief zicht op de kosteneffectiviteit.

Service Level Management
Proces om vitale niveaus van service te definiëren, vastleggen en managen voor geselecteerde IT-assets. Dit proces omvat ook het verifiëren van informatie, wat het daadwerkelijke niveau van service bevestigt.

Overig risicomanagement
Proces om eventuele andere risico's, die niet onder de andere processen vallen, te identificeren en managen. Het bepalen van de effectiviteit van geïmplementeerde risicomanagementprocessen valt onder (maar is niet gelimiteerd tot) dit proces. ISO legt bij de beschrijving van deze Tiers veel verbindingen met processen die betrekking hebben op IT Asset Management in het algemeen. Software assets zijn in enkele gevallen ook direct verbonden met fysieke IT-assets. Gezien deze verbindingen kan het aansluiten op reeds bestaande processen een uitgangspunt zijn, waarmee de software assets op een efficiënte wijze kunnen worden beheerd.

Figuur 2. De SAM-functie binnen een organisatie.
Legenda: groen = personen/afdelingen;
paars = Tier 1; lichtblauw = Tier 2; geel = Tier 3.



Op diverse procesgebieden van SAM kunnen kosten worden bespaard

Vanuit de afdeling Finance wordt aan de afdeling Inkoop een budget beschikbaar gesteld om te voldoen aan de behoeftes van de organisatie en nieuwe contracten af te sluiten. Finance is verder betrokken bij het uitvoeren van kostenanalyses en de allocatie van het softwarebudget binnen de organisatie. Met name het uitvoeren van kostenanalyses is een voorbeeld van optimalisatie, zoals bedoeld in Tier 3. Een ander voorbeeld van optimalisatie in Tier 3 kan de internal audit-afdeling zijn, die periodiek een audit initieert om na te gaan of de SAM-processen op efficiënte wijze worden uitgevoerd, en wat bijvoorbeeld de compliance-positie per leverancier is.

Het SAM-team coördineert deze processen en draagt zorg voor de realisatie van de doelstellingen, zoals vastgelegd in de drie Tiers. Een SAM-team kan, afhankelijk van de omvang van de diverse softwareportefeuilles, een of meerdere licentie-experts hebben. Gezien de complexiteit van licentiemetrieken (denk bijvoorbeeld aan metrieken als *'authorized user single install'*, of per *'processor value unit'*) vergt deze functie noodzakelijke vakkennis om compliant te blijven. Zo hebben met name de grotere organisaties bijvoorbeeld een IBM-, Microsoft-, Oracle-, of SAP-licentie-expert in dienst; niet alleen om compliant te blijven, maar ook om licentieaudits af te handelen, die vanuit de leveranciers periodiek uitgevoerd worden.

CONCLUSIE

Uiteindelijk is het aan de organisatie zelf om het ambitieniveau ten aanzien van SAM te bepalen. De nieuwste ISO biedt organisaties meer vrijheid om zelf hun ambities vast te stellen, en dit zal niet voor elke organisatie de hoogste Tier betreffen. Voor de ene organisatie zal het realiseren van Tier 1 voldoende zijn: het beschikken over betrouwbare data. Van andere organisaties, met grotere softwareportefeuilles en een grote afhankelijkheid van IT, mag men verwachten dat het ambitieniveau hoger gelegd wordt, door SAM-processen te integreren met overige bedrijfsprocessen, en zodoende meer doelstellingen van SAM te realiseren. Door aan te sluiten bij de IT-asset management-norm biedt ISO enkele handvatten om deze procesintegratie soepeler te laten verlopen. Gezien de intrede van cloud-omgevingen naast de bestaande IT-infrastructuur neemt de complexiteit alleen maar toe. Wil een organisatie intern, maar ook naar buiten toe, het vertrouwen uitdragen dat alles onder controle is, zal elke organisatie ambities op het gebied van SAM moeten hebben. Continue aandacht voor softwarelicentie-vraagstukken en -gebruik levert kostenbesparingen op, minimaliseert bedrijfsrisico's en vergroot daarmee het vertrouwen in de IT-omgeving.

Met name het uitvoeren van kostenanalyses is een voorbeeld van SAM-optimalisatie

Literatuur

[GART17] Gartner, *Gartner IT Budget: Enterprise Comparison Tool*, Gartner.com, http://www.gartner.com/downloads/public/explore/metricsAndTools/ITBudget_Sample_2012.pdf, 2017.

[ISO14] ISO/IEC, *ISO/IEC 55000: 2014. Asset management – Overview, Principles and terminology*, 2014, par. 3.2.1.

[ISO17-1] ISO/IEC, *ISO/IEC 19770-5: 2017. Information technology – IT Asset Management – Part 5: Overview and vocabulary*, 2017, p. 11.

[ISO17-2] ISO/IEC, *ISO/IEC 19770-1: 2017: Information technology – IT Asset Management – Part 1: IT asset management systems – Requirements (ISO/IEC 19770-1:2017, IDT)*, 2017, p. vi., p.9, 10,19, 27-30.

[Rudd09] C. Rudd, *ITIL V3 Guide to Software Asset Management*, The Stationary Office, 2009, p. 4.

[SPIC18] Spiceworks, *The 2018 State of IT*, Spiceworks.com, https://www.spiceworks.com/marketing/state-of-it/report/, 2018.

Over de auteurs

L.R. Huijsman MSc RE CISA is zes jaar werkzaam geweest binnen het Contract Compliance Services-team van KPMG Advisory en heeft ervaring met Software Asset Management-adviestrajecten in zowel de financiële als publieke sector. Naast het uitvoeren van adviestrajecten heeft hij uitgebreide ervaring met softwarelicentie-audits voor diverse softwareleveranciers, zoals IBM, Microsoft en Quest. Hij is momenteel werkzaam als Software Asset Management-analist bij CRH.

W.K. Pluim LLB heeft ruim tien jaar ervaring met softwarelicenties en -overeenkomsten en is actief betrokken bij de Software Asset Management-praktijk van KPMG. Voordat hij bij KPMG terechtkwam, heeft hij (inter)nationale teams geleid bij Oracle License Management Services (LMS). De basis van zijn kennis is gelegd op de juridische afdeling van IBM, waar hij jarenlang over de juridische voorwaarden van omvangrijke of afwijkende soft- en hardwarecontracten onderhandelde.