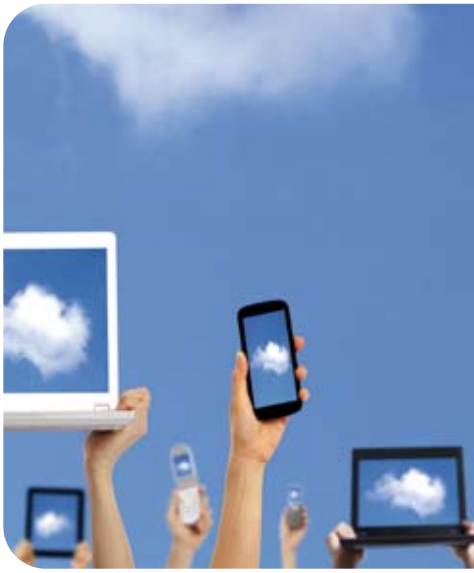
BYO - Bring Your Own

Vergeet techniek, focus op gebruikers



De drie letters BYO staan voor één van de meest besproken trends van deze tijd: 'Bring Your Own'. De crux van het BYO-concept is dat medewerkers met hun eigen device toegang tot verschillende applicaties en bijbehorende data krijgen. Deze applicaties worden zowel vanuit de private als publieke cloud beschikbaar gesteld.

Voordat bedrijven overgaan tot de implementatie van een BYO-concept, is het zaak goed te bedenken wat het doel is en wat de gevolgen zijn. Niet alleen voor het bedrijf zelf, maar ook voor de medewerkers. Qua technologie is vrijwel alles mogelijk, belangrijker is de uiteindelijke invulling en uitvoering van het complete concept.

We schetsen hoe BYO een trend is geworden, bespreken de technologische ontwikkelingen die het mogelijk maken en gaan in op de veranderde mindset van gebruikers. Vervolgens komen de juridische en fiscale consequenties voor bedrijven aan de orde.

PQR
Eenvoud in ICT

1 BYO is niet nieuw

BYO is niet nieuw. Hieraan ten grondslag ligt de 'Consumerization of IT' en de 'It's about ME-attitude' van gebruikers die zich als consumenten gedragen en zo behandeld willen worden. De grenzen tussen zakelijk en privé vervagen. De afgelopen jaren heeft de ontwikkeling van mobiele devices een vlucht genomen; er zijn nieuwe vormen, zoals tablets, toegevoegd en omarmd. Applicaties worden via internetwinkels ter beschikking gesteld, gratis en tegen betaling, wat ervoor heeft gezorgd dat consumenten veel makkelijker gebruik van IT-middelen kunnen maken.

De manier waarop applicaties worden ontworpen, gebouwd, gedistribueerd, geüpdate en beheerd heeft zo'n vlucht genomen, dat bedrijven en consumenten probleemloos van deze applicaties gebruik kunnen maken. IT wordt als dienst in private en publieke clouds aangeboden en dit levert een groot aantal nieuwe mogelijkheden op: AnyWhere, AnyPlace, AnyDevice, AnyUser, AnyContent en AnyTime toegang tot apps, tot netwerken, tot informatie. Gebruikers kunnen hun digitale activiteiten voor een groot deel zelf regelen. Zij creëren hun eigen Personal Cloud die bestaat uit hun eigen applicaties, services, content en data.

Mobiele devices in combinatie met beschikbare IT-diensten, vervullen tegenwoordig veel taken van Personal Computers. De Personal Computer wordt zelfs meer en meer vervangen door de Personal Cloud. Op ieder moment van de dag en afhankelijk van locatie, tijd, device en content, kan elk device de rol van 'belangrijkste/primaire' computer van de gebruiker innemen. Het scherm geeft toegang tot de content; de grootte van elk scherm bepaalt welke toepassingen op welke soort device gebruikt worden. Naast schermgrootte is de technologie die het device ondersteunt erg belangrijk. Zo wordt een 'simpele' mobiele applicatie met GPS, camera, Gyro en 3G/LTE een Rich Internet Applicatie.

2 Waarom wil iedereen juist nu overstappen op een BYO-concept?

Consumerization (MeMeMe) en het loslaten van de vaste werkplek, "the world is my workplace" vragen om aanpassingen van de traditionele manier waarop IT aan gebruikers wordt aangeboden. De brede acceptatie en penetratie van tablets, smartphones, apps en connectivity hebben ervoor gezorgd dat vrijwel iedereen altijd 'connected' is en van de meest actuele informatie gebruik kan maken. De manier waarop mensen communiceren via social media heeft gezorgd voor nieuwe communicatiekanalen die gebaseerd zijn op AnyWhereAccess. Vertalen we dit naar IT trends, dan zien we als belangrijkste aanjagers van BYO: Mobility, Cloud, Social Media, AllwaysOn en de 'ik-cultuur'.

Vroeger was het de IT-afdeling die bepaalde hoe en met welke apparatuur en infrastructuur werd gewerkt, tegenwoordig is het steeds vaker de gebruiker die bepaalt. Deze Consumerization of IT heeft alles te maken met een verandering van mindset. Gebruikers van nu willen zelf 'in control' zijn, vrijheid en keuze hebben en willen niet alles in hapklare brokken van IT te ontvangen. De gebruiker denkt dat alles kan, IT moet het faciliteren. Dat laatste klopt als het gaat om de infrastructuur en de beveiliging. BYO heeft echter ook direct te maken met HR, Finance en Legal. Beleid, richtlijnen en regelgeving zullen door deze afdelingen opgesteld, gedicteerd, geïmplementeerd en gecontroleerd (in- en extern) moeten worden.

Ook de begrippen thuis en kantoor zijn minder stringent geworden: werk is niet meer locatiegerelateerd, werk gaat om de inhoud. IT is in zo'n geval aan de wensen van de gebruiker aangepast. Met duidelijk zichtbare gevolgen, voor zowel individuen – in hun rol van zakelijke gebruiker én van consument – als voor beheerders van IT-omgevingen. Van de laatste groep wordt met de opkomst van BYO een nóg klantgerichtere benadering verwacht; beheerders gaan meer en meer als service manager acteren.

AnyWhereAccess

Parallel aan de ontwikkeling van Bring Your Own willen steeds meer mensen altijd en overal kunnen werken. Deze trend 'AnyWhereAccess' levert een nog grotere uitdaging op. De traditionele manier van werken, support geven, beheer en beveiliging moet opnieuw onder de loep worden genomen. Bedrijven moeten een visie formuleren over het veilig beschikbaar stellen van applicaties en desktops, en een strategie bepalen die hierop gebaseerd is. Daarvoor moeten zij goed inventariseren wat er is, wat nodig is, waarom dat nodig is en of het oplevert wat ervan wordt verwacht. Bij BYO gaat het om toegang tot Windows-applicaties, Web-/SaaS-applicaties en Rich Internet/Rich Mobile applicaties. Deze drie soorten applicaties kunnen uit publieke en private clouds komen, waarbij Single-Sign-On (SSO) en federatie worden samengebracht in een persoonlijke en aangepaste interface die deze zaken regelt.

3 Virtuele Desktop: duidelijke businesscase

Het aanbieden van applicaties kan op meerdere manieren; desktopvirtualisatie of Virtual desktop Infrastructure (VDI) is er één van. De Server Hosted Desktops die hiermee ontstaan, geven toegang tot gecontroleerde en veilige applicaties op een werkplek of device dat zelf niet beheerd wordt. De controle ligt in dit geval op de gateway (toegang) en centrale uitvoering van de applicaties en niet op het device.

Implementatie is echter geen eenvoudig project. Het heeft impact op de complete ICT-infrastructuur.

Wie desktopvirtualisatie overweegt, moet zichzelf afvragen hoe zijn huidige desktopstrategie eruitziet en wat hij met een VDI-strategie wil bereiken. Vervolgens kan gefundeerd een technologie worden gekozen en kunnen de features van verschillende producten worden vergeleken.

De volgende vragen helpen bij het definiëren van een duidelijke businesscase:

- Hoe gebruiken uw medewerkers werkplekken? Is er behoefte aan desktopvirtualisatie? Waarom desktopvirtualisatie? Wat wilt u bereiken? Gaat het erom dat werknemers hun taken kunnen vervullen (bedrijfsenabler)? Of draait het primair om kosten en verlaging van de total cost of ownership?'
- Kijkt u naar een tactische of strategische oplossing? Welk probleem wilt u oplossen?
- Wat zijn de belangrijkste pijlers voor de optimale virtuele desktop?
- Hoe faciliteert u roaming/flexibele en mobiele gebruikers binnen uw bedrijf?
- Hoe gaat u om met het beschikbaar stellen van desktops en applicaties als een gebruiker verschillende toegangsscenario's heeft? Hoe levert u applicaties aan gebruikers in een Bring Your Own- of Choose Your Own-scenario?
- Hoe voorkomt u dat medewerkers bij een defect device niet meer productief zijn?
- Wat verwachten de gebruikers van de virtuele desktop (vDesktop)? Welke devices ondersteunt u en welke invloed hebben deze op de gebruikerservaring?
- Hoe kunnen gebruikers met al hun apparatuur veilig toegang krijgen tot en gebruikmaken van het netwerk? Welke invloed hebben secure access- en secure network-oplossingen op mobiele devices als ze verbinding maken met de vDesktop? Moet u deze endpoints eigenlijk beheren?
- Vormt het in gebruik stellen en beheren van het software-image onderdeel van de VDI-strategie? Welke rol speelt user environment management hierin?
- Hoe ontwerpt, bouwt en onderhoudt u het Windows-gebruikersprofiel?
- Houdt u rekening met de context (locatie, tijd, device, security)?
- Laat u de gebruiker zelf applicaties installeren?
- Wat is de invloed op prestaties en storage wanneer u applicatievirtualisatie in combinatie met VDI gebruikt? Hoe beïnvloedt de impact op storage de businesscase?

- Op welk type images richt u zich? Wat is de impact op storage en beheer?
- Hoe schaalt u de VDesktop en bijbehorende infrastructuur, en bent u bekend met de best practices voor het optimaliseren van de vDesktop?
- Welke invloed hebben prestaties en bandbreedte op de netwerkinfrastructuur (LAN, WAN, WLAN)?
- Hoe stelt u het profiel en de werkomgeving van de gebruikers samen?
- Hoe zit het met licenties voor bijvoorbeeld besturingssysteem, clienttoegang en applicaties? Dit heeft zeker bij invoering van BYO nogal wat uitdagingen: bedrijven zullen heel goed naar de wijze van licentiering van desktop, Office en overige licenties moeten kijken.
- Maakt u een back-up van de vDesktop (en wilt u hem kunnen herstellen)?
- Hebt u antivirussoftware nodig? Binnen de virtuele machine zelf of als servicemodule op de hypervisor?
- Heeft de IT-organisatie genoeg ervaring om deze technologie te ondersteunen en te onderhouden?
- Hoe staat het met de kennis en kunde binnen de IT-afdeling?

4 Risicoprofielen van de vijf benaderingen van BYO-werkplekken

In een BYO-situatie bepalen medewerkers hoe zij hun werkplek en applicaties inzetten om hun werk te kunnen doen. Een bedrijf wil medewerkers ondersteunen en stimuleren en een werkplek die voor zijn of haar functie het meest geschikt is, aanbieden. De IT-afdeling moet hier echter wel in kunnen faciliteren en niet alleen de functionele werking, maar tevens de controle en beveiliging waarborgen.

BYO is niet voor iedereen geschikt. Niet voor iedere medewerker, maar ook niet voor ieder bedrijf. Daarom zijn er verschillende benaderingen voor het aanbieden van een werkplek gedefinieerd. De mate van zelfredzaamheid, de behoefte aan controle, flexibiliteit en vrijheid bepalen welk concept het meest geschikt is.

Voor IT-managers is het concept 'This is the device', oftewel 'Hier is je eigen werkplek' het meest ideaal. De IT-manager of IT-medewerker bepaalt welke hardware de medewerkers tot hun beschikking krijgen. Er worden geen uitzonderingen op de regel gemaakt. De controle van apparatuur en gegevens is optimaal! De (keuze)vrijheid van de gebruiker is klein en de beslissingen omtrent zijn IT worden voor hem gemaakt.

Hier lijnrecht tegenover staat het min of meer anarchistische 'On Your Own' idee: alles kan, alles mag; er bestaan geen restricties als het gaat om gebruik en aanschaf van hardware en applicaties. Gebruikers hebben maximale vrijheid en er wordt van hen een grote mate van zelfredzaamheid verwacht. Een bedrijf verliest in deze situatie de controle. Met alle risico's van dien, bedrijfsgegevens worden immers op het device gebruikt en de mate van beveiliging ligt geheel in handen van de gebruiker.

Er bestaan ook tussenvormen: 'Choose Your Own' (CYO), 'Kies je eigen werkplek', waarbij medewerkers kunnen kiezen uit een lijst van gespecificeerde hardware en bepaalde ondersteuning van services hierop, 'Bring Your Own' (BYO) of 'Breng je eigen werkplek mee', waarbij de werknemer hardware uitzoekt die de werkgever betaalt en 'Buy Your Own' of 'Betaal je eigen werkplek', met complete vrijheid in de keuze van hardware en bijna geen restricties.

Verwachtingen gebruikers IT en andersom

Zodra een bedrijf overstapt op een BYO-concept, gaan beveiliging en het managen van de verwachtingen een nog belangrijkere rol spelen. Controle en beveiliging van data en apparatuur vinden steeds vaker op het netwerk plaats: Mobile Device, maar vooral Mobile Application en Data Management worden steeds belangrijker. Hiermee zijn bedrijfsgegevens bij verlies of diefstal van een device beschermd; zo is het bijvoorbeeld mogelijk om zakelijke gegevens op afstand te verwijderen.

Gebruikers krijgen een actieve rol: zij erkennen beveiligingsrisico's die samenhangen met deze manier van werken en passen hun gedrag aan. IT ondersteunt hen hierin door services te leveren die de risico's verkleinen.

Bedrijven moeten een beleid ontwikkelen met de volgende aandachtspunten:

- Waarborgen van veilige omgang met bedrijfsgevoelige en privacygevoelige gegevens.
- Centrale sturing op configuratie, uitzetten van de software en beheer.
- Richtlijnen rond toegang, updates en veiligheid van apparaten en software.

Het is belangrijk om duidelijk te formuleren wat gebruikers van IT mogen verwachten en vice versa: de uitleg van de voor- en nadelen van de aangeboden functionaliteit en daarnaast de verwachtingen rondom zelfredzaamheid, vrijheid en controle.

5 Overheid en BYO – wet- en regelgeving: juridisch

Naast de praktische IT-kant van een BYO-implementatie hebben organisaties ook te maken met juridische en fiscale wet- en regelgeving. De komende twee paragrafen gaan in op deze aspecten, maar hebben geen rechtsgeldigheid. Wel geven zij een overzicht van de huidige mogelijkheden. Voor de laatste stand van zaken en adviezen hieromtrent verwijzen wij u graag door naar juristen en fiscalisten.

Juridisch

Wanneer een bedrijf een BYO-concept invoert, zijn er een aantal zaken rond aansprakelijkheid die van belang zijn. Want wat doe je als iemand op zijn privélaptop illegale software gebruikt, maar deze laptop ook inzet voor zijn werk? Wat als er vanaf de privélaptop virussen op het bedrijfsnetwerk komen – of omgekeerd? Is het bedrijf aansprakelijk voor beschadigde of gecrashte privélaptops als de oorzaak tot het bedrijf te herleiden is?

BYO is natuurlijk een nieuw concept; alle ins en outs van aansprakelijkheid en BYO zijn nog niet uitgekristalliseerd. Het Burgerlijk Wetboek geeft de volgende richtlijnen. De werknemer en werkgever moeten zich "goed" naar elkaar gedragen (art. 7:611 BW). De werkgever mag daarbij redelijke instructies geven over hoe het werk moet worden uitgevoerd (art. 7:660 BW).

De werkgever kan bijvoorbeeld de werktijden eenzijdig vaststellen en kan bepalen dat wachtwoorden minstens 15 tekens lang moeten zijn. De werknemer moet dergelijke instructies opvolgen. Werkgevers doen dit vaak met een arbeidsreglement, en het is dus een misverstand dat dit geaccordeerd moet worden of dat zulke regels in een arbeidsovereenkomst dienen te staan.

Omdat de werkgever zo veel zeggenschap heeft, is hij in principe altijd de aansprakelijke partij. Zo bepaalt de wet dat de werkgever de "gereedschappen" waarmee het werk wordt gedaan, zo moet inrichten dat de werknemer daar redelijkerwijs geen schade door zou kunnen lijden (art. 7:658 BW).

Dit geldt ook voor het bedrijfsnetwerk, en daarmee is de werkgever dus aansprakelijk als virussen of andere rommel schade berokkent aan het privé device van de werknemer. Mits de werkgever redelijkerwijs had kunnen voorkomen dat deze schade zou optreden.

Omgekeerd is de werknemer naar de werkgever toe nooit aansprakelijk, tenzij de schade een gevolg is van zijn opzet of bewuste roekeloosheid (art. 7:611 BW). Dit geldt ook naar derden toe (art. 6:170 BW): de werkgever is aansprakelijk als een privélaptop door een fout van derden wordt beschadigd.

Wel moet sprake zijn van schade die binnen de uitvoering van de arbeidsovereenkomst valt. Een werknemer die met een eigen device bedrijfsmail leest, waarna een Outlookworm op dat device een bedrijfsgeheim doormailt naar Rusland, handelt binnen de uitvoering want hij was werkmail aan het afhandelen. Een werknemer die games gaat zitten downloaden van Usenet, handelt niet binnen de arbeidsovereenkomst want dat behoort niet tot zijn werk. Hij is dus zelf aansprakelijk voor die schade.

Bij illegale bedrijfssoftware ligt het anders. Een werknemer die een gekraakte Photoshop (of een legitieme Windows 7 Home Edition, die immers niet zakelijk mag worden gebruikt) op een eigen device inzet bij het werk, is bezig met de uitvoering van zijn werk. En dan ligt de aansprakelijkheid voor de missende licenties bij de werkgever. Die moet zorgen dat de licenties van de, op de het privé device aanwezige, software het gebruik op het werk toestaan. Bij invoering van BYO moeten bedrijven heel goed naar de wijze van licentiering van desktop, Office en overige licenties kijken, aangezien daar nogal wat haken en ogen aan kunnen zitten.

6 Overheid en BYO – wet- en regelgeving: fiscaal

Computer of telefoon?

Hoe moeten BYO-kosten verwerkt worden? Wat zegt de belastingdienst hierover? Allereerst is het belangrijk vast te stellen of het privé device onder 'computers en vergelijkbare apparatuur' of 'internet, telefoons en andere communicatiemiddelen' valt. De regels voor een onbelaste vergoeding of terbeschikkingstelling van communicatiemiddelen, zoals een smartphone, wijken namelijk af van de regels voor computers. Om te bepalen onder welke regels dit soort apparaten - zoals tablets - vallen, kan de werkgever naar de schermgrootte kijken. Smartphones en dergelijke apparaten met een beeldscherm (diagonaal) van maximaal 7 inch (17,78 cm) zijn communicatiemiddelen, is het scherm groter, dan spreken we van computers.

Werkkostenregeling (WKR) computers

Momenteel wordt er in het 'Handboek Loonheffingen' van de Belastingdienst niet vermeld hoe het gebruik van computers buiten de werkplek van de werknemer in de werkkostenregeling (WKR) moet worden opgenomen (paragraaf 18.8 van het 'Handboek Loonheffingen 2011' onder 'U maakt gebruik van de werkkostenregeling'). Werkgevers kunnen werknemers onbelast een computer en vergelijkbare apparatuur ter beschikking stellen als de werknemer aan de volgende twee voorwaarden voldoet:

1. De werknemer gebruikt de apparatuur voor 90% of meer zakelijk.
2. De werknemer gebruikt de apparatuur (gedeeltelijk) op de werkplek.

Als de werknemer niet aan deze voorwaarden voldoet, wordt de factuurwaarde van de computer en vergelijkbare apparatuur (inclusief BTW) bij het loon van de werknemer opgeteld en zal er belasting over moeten worden betaald. De werkgever kan dit loon ook als eindheffingsloon onderbrengen in de vrije ruimte – waarbij de zogenoemde gebruikelijkheidstoets bepalend is. Dit houdt in dat de vergoedingen en verstrekkingen die als eindheffingsloon worden aangemerkt, niet meer dan 30% mogen afwijken van wat in vergelijkbare omstandigheden gebruikelijk is.

Het kan bijvoorbeeld voorkomen dat een werknemer een computer of tablet cadeau krijgt van zijn leverancier. De werkgever kan de apparatuur dan volledig in de vrije ruimte onderbrengen. Maximaal één werkplek komt in aanmerking voor belastingvoordeel; er is sprake van een werkplek als het scherm van het device groter is dan 7 inch.

Communicatiemiddelen

De vergoedingen of verstrekkingen van internet, telefoon en dergelijke communicatiemiddelen (bijvoorbeeld een smartphone) zijn onbelast, als werknemers deze middelen voor meer dan 10% zakelijk gebruiken. Datzelfde geldt voor een 2e telefoonaansluiting. Als de werkgever deze communicatiemiddelen zelf aan zijn werknemers ter beschikking stelt, gelden dezelfde regels.

Als werknemers deze communicatiemiddelen voor 10% of minder zakelijk gebruiken, is de vergoeding, verstrekking of terbeschikkingstelling loon voor alle loonheffingen. De waarde van dit loon wordt als volgt bepaald:

- Bij vergoeding is de hele vergoeding loon.
- Bij verstrekking is de waarde van de verstrekking in het economische verkeer loon.
- Bij terbeschikkingstelling zijn de kosten die de werkgever maakt loon. Dit zijn onder andere de abonnements- en afschrijvingskosten.

Let op!

In de volgende situaties is er geen sprake van een werkplek:

- De werknemer werkt onderweg. Hij mailt bijvoorbeeld in de trein of de bus of schrijft een artikel in een horecagelegenheid. In deze situaties is de werkgever niet arboverantwoordelijk. Voor de voorzieningen die de werknemer onderweg gebruikt, geldt geen nihilwaardering.
- De werknemer werkt in een werkruimte in zijn eigen woning, woonboot, vakantiewoning of woonwagen. Bij de woning van de werknemer hoort ook de garage, het tuinhuis en dergelijke.
- De omstandigheden van de werknemer wijzigen. Dat is bijvoorbeeld het geval bij een overplaatsing (de oude werkplek is dan geen werkplek meer), blijvende arbeidsongeschiktheid of het einde van de dienstbetrekking.

Als de werknemer zijn eigen mobiele telefoon gebruikt, kan de werkgever het telefoonabonnement belastingvrij ter beschikking stellen bij een zakelijk gebruik van meer dan 10%. Een vergoeding voor het telefoonabonnement is belast loon. Maar dit loon kan ook als eindheffingsloon worden ondergebracht in de vrije ruimte.

*Bron: http://www.belastingdienst.nl – wet- en regelgeving is aan verandering onderhevig – zie altijd de website van de belastingdienst.

Conclusie: een doordacht plan

Het mag duidelijk zijn, dat BYO voor zowel gebruikers, IT als de hele organisatie veel consequenties heeft. Het is dan ook belangrijk het gewenste resultaat helder te formuleren en een doordacht plan op papier te zetten. Vanuit meerdere invalshoeken. Zo is het handig om met de verschillende groepen gebruikers hun verschillende rollen en hun IT-behoefte te definiëren en met hen te onderzoeken welke businessprocessen door IT nog beter ondersteund kunnen worden. En natuurlijk moet ook gekeken worden, wat binnen het bedrijf mogelijk is qua investeringen in tijd, geld en mankracht.

Om dit soort scenario's goed te kunnen beoordelen, is het verstandig zelf de oplossingen en bouwstenen voor uw organisatie kritisch onder de loep te nemen. Stel de vragen 'Wat is de waarde van 'IT als dienst' voor mijn organisatie en voor de gebruikers? Waarom voegen we iets toe? Wat verwacht de gebruiker van IT om zijn businessproces beter te kunnen ondersteunen?'. Denk na over het strategische en tactische nut en beoordeel of het zinvol is. En kijk dan vooral naar de toepassingen voor uw gebruikers!

Concreet

Vergeet technologie, focus op de eindgebruiker! Denk in toegangsscenario's en 'use cases'. Concreet betekent dat voor u een exercitie waarin u de wensen en eisen van de gebruiker, én de mogelijkheden vanuit de IT-afdeling, vastlegt.

Het lijkt een open deur, maar begin bij het begin. Doe wat voor uw specifieke situatie het beste is, stel een doel en definieer een stappenplan om dat doel te bereiken.

Zo'n stappenplan moet in ieder geval de volgende componenten bevatten:

- inventarisatie van de wensen en eisen van de gebruiker;
- inventarisatie van de mogelijkheden;
- bepalen van de rolprofielen
- toekennen van rechten, autorisaties voor applicaties
- bepaal hoe u beheer en beveiliging regelt etc.

Vergeet daarbij niet de gebruiker bewust te maken van zijn verantwoordelijkheden en van de fiscale en juridische gevolgen van de verschillende concepten.

Aan de slag met BYO

Wij helpen u graag! Neem voor meer informatie contact op met Bas ter Heurne van PQR, telefoon 030-6629729 of e-mail info@pqr.nl. De digitale versie van deze BYO-brochure kunt u downloaden via www.PQR.com.

PQR B.V. ■ Rijnzathe 7 ■ 3454 PV De Meern
Tel. 030 662 97 29 ■ Fax 030 666 59 05 ■ info@pqr.nl ■ www.PQR.com