ACHTER DE WOLKEN...

# Assurance over de cloud

Het verplaatsen van dataopslag en/of verwerking naar de cloud brengt altijd risico's met zich mee. Gelukkig zijn er al diverse 'assurance-producten' op de markt.

TEKST: ELLY STROO CLOECK EN GERARD BOTTEMANNE* | BEELD: DREAMSTIME

Het artikel 'Donkere wolk' in het meinummer van Accountant, belichtte vooral de juridische aspecten van continuïteitsrisico's in de cloud. Er zijn ook positieve zaken te melden over de risico's van cloud-computing. Zo zijn er al 'assurance-producten' op de markt die zich onder meer richten op de volgende cloud-risico's:

- afhankelijkheid van een aanbieder (data portabiliteit);
- ongeautoriseerde toegang tot gegevens (integriteit en vertrouwelijkheid);
- gebrek aan bedrijfszekerheid van de gegevensverwerking (continuïteit).

Kijkend naar deze producten en andere maatregelen, is het gerechtvaardigd om te stellen: achter de wolken schijnt de zon.

## ASSURANCE-RAPPORT

Veel (cloud-)outsourcing-leveranciers, ook de kleinere, leveren een assurance-rapport op basis van ISAE 3402. Han Boer, zelfstandig adviseur op het gebied van assurance bij businessprocessen in serviceorganisaties, schetst de achtergrond: "Dit rapport is gebaseerd op IFAC-standaard ISAE 3402 en vervangt sinds medio 2011 het bekende SAS 70-rapport. In Nederland is de IFAC-standaard door de NBA overgenomen onder de naam NV COS 3402. NOREA, de beroepsvereniging voor IT-auditors, heeft het omarmd met de naam Richtlijn 3402."
Volgens Boer is het uniek dat ook de AICPA ("de Amerikaanse NBA, zeg maar") de standaard inhoudelijk gezien in vrijwel ongewijzigde vorm heeft overgenomen. "De formele naam van de standaard in Amerika is SSAE 16. De AICPA heeft de standaard met de werknaam SOC 1, (Service Organisation Control-report ) in de markt gezet. De oude Amerikaanse SAS 70-standaard is hiermee vervangen door één internationale standaard die materieel gezien, ongewijzigd wordt gevolgd of is overgenomen in de lokale set van audit- en assurance-standaarden."

'VEEL (CLOUD-)OUTSOURCING-LEVERANCIERS, OOK DE KLEINERE, LEVEREN EEN ASSURANCE-RAPPORT OP BASIS VAN ISAE 3402.'

## ZEKERHEID

Welke zekerheid kan een klant van een cloud-leverancier nu aan zo'n rapport ontlenen? Temme Sikkema, registeraccountant en IT-auditor bij Hut & Co legt uit: "In een ISAE 3402/SOC 1-assurance-rapport is een uitgebreide beschrijving opgenomen van specifieke, door het management van een cloud-leverancier geformuleerde beheersingsdoelstellingen omtrent financiële verslaglegging. En ook welke controls zijn geïmplementeerd om die doelstellingen te behalen.
De accountant geeft assurance over de getrouwheid van de beschrijving, de mate waarin de controls een bijdrage leveren aan de geformuleerde doelstellingen en of deze effectief hebben gewerkt gedurende de verslagperiode. Het is dus geen verklaring, geen certificaat en geen garantiebewijs!"
Aan de andere kant, vervolgt Sikkema, heeft (de accountant van de) cloud-klant nu wel informatie over de werking van de controls in de cloud: "Het is wél de bedoeling dat de klantorganisatie deze stukken leest en mogelijke resterende risico's herkent en compenseert. De grotere cloud-leveranciers leveren ISAE 3402-rapporten al langer en met een hoge frequentie. Maar ook in het mkb wordt SOC 1 inmiddels veel toegepast."

## SOC 2 EN SOC 3

Sinds kort worden ook de AICPA-rapportages SOC 2 en SOC 3 gebruikt. In Nederland zijn deze nog niet zo gebruikelijk, wat hopelijk maar tijdelijk is, want deze zijn heel nuttig. Han Boer onderschrijft dit: "Een SOC 2-rapport geeft inzicht in één, of combinaties, van de volgende aspecten: beveiliging, beschikbaarheid, integriteit van de verwerking, vertrouwelijkheid en

## KEURMERK ZEKER ONLINE

**In Nederland wordt gewerkt aan het keurmerk 'Zeker Online' dat zich richt op boekhoudsoftware via het cloud-model. Zeker Online is een gezamenlijk initiatief van de markt en de Belastingdienst, gefaciliteerd door ECP, het platform voor privaat/publieke samenwerking. Ook accountants en auditors zijn betrokken bij dit initiatief. Positief voor zowel accountants als hun klanten is dat binnen Zeker Online wordt gewerkt aan een normenkader dat gericht is op het verschaffen van 'zekerheid', qua beveiliging, continuïteit en functioneren. De verwachting is dat in de loop van 2013 het eerste normenkader een feit is, waarna boekhoudsoftware via de cloud onderworpen kan worden aan het normenkader. Informatie over Zeker Online is te vinden op http://www.zeker-online.nl/.**

privacy. De rapportagevorm komt overeen met de vorm van een ISAE 3402 (SOC 1)-rapport."
Het fundamentele verschil is dat de beheersingsdoelstellingen vooraf zijn gedefinieerd, stelt Boer: "Deze worden de 'Trust service principles and criteria' genoemd, een soort normenkader dus. Een SOC 2-rapport is primair bedoeld voor de klant van de cloud-leverancier om afhankelijk van de gekozen criteria inzicht te geven in de getroffen maatregelen. Wie om een SOC 2-report *security en availability* vraagt, weet precies wat hij krijgt."
Een SOC 3-rapport is bedoeld voor een breed publiek, in tegenstelling tot een SOC 1- of 2-rapport, die uitsluitend bestemd zijn voor de klanten die van het in scope zijnde systeem hebben gebruikgemaakt. De SOC 3-rapportage is veel korter en kan, met het officiële SOC 3-logo worden gepubliceerd, als een zegel met daarin het (uiteraard positieve) oordeel van de accountant.

**Zie ook Accountant.nl/ Vaktechniek**

## MKB EN SOC 1

**Veel kleinere datacenters en hostingpartijen laten hun belangrijke beheerprocessen al auditen volgens de SOC 1-standaard. Maar ook SaaS-leveranciers, bijvoorbeeld online salarisverwerkers, laten ISAE 3402-opdrachten uitvoeren. Vaak is de *trigger* hiervoor een (corporate) klant die een SOC 1-rapport eist, maar meer en meer is SOC 1 ook in het mkb een *competitive edge* geworden. Temme Sikkema van Hut & Co, een klein accountantskantoor: "Een voorbeeld hiervan is Multrix, een cloud-leverancier die wij van een SOC 1-rapport voorzien. De klanten van Multrix zijn, naast grote ondernemingen, ook kleine accountantskantoren, zorginstellingen en onderhoudsbedrijven."**

## VIER TIPS

- **Check regelmatig (in elk geval eens per jaar) de financiële positie van een softwareleverancier en ga na of het aantal klanten groeit, juist stabiel blijft of zelfs afneemt. Dit laatste is aanleiding om extra alert te zijn.**
- **Ga na of er een gebruikersvereniging is van de software. Een exit-strategie afspreken met gelijkgestemden is een goed onderwerp voor een gebruikersgroep.**
- **Ga na of de leverancier steeds tijdig rekening houdt met nieuwe ontwikkelingen. Voor boekhoudsoftware is dit bijvoorbeeld SEPA en het aanleveren van btw-aangiftes en ICP-opgaves via SBR. Als de leverancier geen SEPA-compliant software beschikbaar heeft op 1 februari 2014 kan vanaf dat moment geen betalingsverkeer meer worden afgehandeld via deze software.**
- **Wie overweegt over te stappen naar andere software, doet er goed aan vóór aanschaf te informeren naar de exit-strategie bij de huidige softwareleverancier. De exit-strategie willen regelen na opzeggen van een contract, geeft een minder sterke positie.**

'OM OVER TE STAPPEN NAAR EEN ANDERE SOFTWARELEVERANCIER MOET DE VOLLEDIGE BOEKHOUDING VAN MINIMAAL DE AFGELOPEN ZEVEN BOEKJAREN BESCHIKBAAR BLIJVEN.'

Er zijn wel wat randvoorwaarden, zo mogen er geen beperkingen in het oordeel zijn en mogen er geen belangrijke procesonderdelen van de beoordeling zijn uitgesloten (een *carve out*).
Voor de gebruiker is een SOC 2, door de uitgebreide informatie, van veel grotere waarde dan een SOC 3-rapport. Voor een cloud-leverancier kan het, door de vrije publiciteit, net omgekeerd liggen. De gehanteerde principes en criteria zijn voor beide rapporten gelijk. Op basis van bovenstaande rapporten kunnen sommige cloud-risico's bij de cloud-leverancier als beheerst worden beschouwd. Maar wat als er overgestapt moet worden naar een andere leverancier?

### EXIT-STRATEGIE

Vendor-lock-in, volledig afhankelijk zijn van een leverancier doordat deze 'eigen' opslag of verwerkingssoftware gebruikt, is contractueel te ondervangen door te bepalen dat de leverancier open standaarden moet gebruiken, zo staat in het eerdergenoemde artikel 'Donkere wolk'. Hierover moet echter niet te licht worden gedacht: soms is het gewoon niet mogelijk om de beschikking te krijgen over alle data die moet worden meegenomen. Het werken met een open standaard als XBRL in online-boekhoudprogramma's wil niet zeggen dat alle boekhouddata in XBRL aanwezig zijn. En die zijn natuurlijk wel nodig om een boekhouding te kunnen reproduceren.
Om over te stappen naar een andere softwareleverancier moet de volledige boekhouding van minimaal de afgelopen zeven boekjaren beschikbaar blijven. Dit laatste is mogelijk op onder meer de volgende manieren (de exit-strategie):

1. De huidige boekhoudsoftware blijft toegankelijk voor raadplegen; dit brengt mogelijk kosten met zich mee. Soms is het bij lokale boekhoudsoftware mogelijk de oude software nog op te starten met een systeemdatum in het verleden. Stem af met de leverancier welke mogelijkheden er zijn en tegen welke condities (kosten) dit mogelijk is.
2. Gegevens uit de huidige boekhouding worden volledig geconverteerd naar de nieuwe boekhoudsoftware. Stem wel vooraf af welke kosten hiermee zijn gemoeid .
3. Gegevens uit de huidige boekhouding worden weggeschreven naar pdf-documenten, Excel of een ander leesbaar formaat. Afdrukken op papier is ook een optie, maar niet de meest voor de hand liggende.

'MEER EN MEER IS SOC 1 OOK IN HET MKB EEN COMPETITIVE EDGE GEWORDEN.'

Als gekozen wordt voor optie twee of drie is het raadzaam de inspecteur van de Belastingdienst daarbij te betrekken en goedkeuring op papier te krijgen, om te voorkomen dat een paar jaar later alsnog problemen ontstaan bij een belastingcontrole. Het gaat hier om boekhoudsoftware, maar dit geldt uiteraard ook voor andersoortige software, zoals salarissoftware, dossierbeheer en cliëntportalen.
Als een cloud-leverancier failliet gaat is het van groot belang, in elk geval de duur die nodig is om over te gaan naar een ander systeem met behoud van de gegevens, te kunnen beschikken over de software om een van de bovenstaande exit-strategieën uit te voeren Dit laatste moet vooraf contractueel afgestemd worden met de cloud-leverancier. Dit is een *active escrow*-bepaling. □

**Noot**

** Elly Stroo Cloeck is senior beleidsmedewerker a.i. Beroepsontwikkeling en Beleid NBA en Gerard Bottemanne is eigenaar van onderzoeksbureau GBNED.*