Third-partymededelingen: de ervaringen van de gebruikersorganisaties

Mw. drs. S. van der Eijk-van Eck en drs. K.H.G.J.M. Ho RE RA

Het begrip third-partymededeling (TPM) is onder IT-auditors inmiddels een redelijk ingeburgerd begrip. In deze kringen heeft iedereen wel een idee wat een TPM inhoudt en welk doel zij dient, alhoewel nog wel verschillen van inzicht bestaan omtrent definities, mate van zekerheid en wijze van rapportage. Buiten IT-auditingland begint de bekendheid van het begrip TPM te groeien, zowel onder IT-serviceproviders als hun klanten (gebruikersorganisaties). Deze laatste groep kan – samen met hun externe accountant – worden beschouwd als de primaire doelgroep van een TPM. Omdat het voor zowel IT-serviceproviders als IT-auditors interessant is te weten hoe gebruikersorganisaties een TPM ervaren en in hoeverre een TPM voor hen een toegevoegde waarde heeft, is een aantal gebruikersorganisaties[1] over dit onderwerp geïnterviewd. De resultaten van deze interviews zijn verwerkt in dit artikel.

Inleiding

De afgelopen jaren is in Nederland bij bedrijfsleven en overheid een trend te signaleren om de zelf uitgevoerde activiteiten terug te brengen tot die activiteiten die behoren tot de corebusiness van de organisatie. Niet alleen activiteiten als catering, schoonmaak en transport, maar ook grote delen van de automatisering worden niet tot deze corebusiness gerekend en worden uitbesteed. Hierdoor ontstaat een grote afhankelijkheid van een externe partij voor wat betreft de kwaliteit van de uitbestede activiteiten, hetgeen bij incidenten ernstige gevolgen kan hebben voor de eigen bedrijfsvoering.

De betrouwbaarheid en continuïteit van de uitbestede dienstverlening heeft voor een aantal organisaties een dermate grote invloed op het primaire proces, dat deze organisaties en hun externe accountant niet meer kunnen en durven te vertrouwen op de 'blauwe ogen' van de accountmanager van hun leverancier (serviceprovider). Een onafhankelijke en onpartijdige instantie zal na onderzoek zekerheid moeten verschaffen over de uitbestede activiteiten en hierover moeten rapporteren. Deze rapportage kennen de meeste mensen onder de naam third-partymededeling.

> Bij uitbesteding van diensten zijn de 'blauwe ogen' van de leverancier veelal een te smalle basis voor vertrouwen.

In de dagelijkse praktijk wordt in de meeste gevallen de term third-partymededeling gehanteerd, maar bewoordingen als third-partyverklaring, third-party-announcement of 'onafhankelijk oordeel' komen ook voor. Teneinde de eenduidigheid te bevorderen wordt in dit artikel de meest gebruikte term gehanteerd, te weten third-partymededeling, verder afgekort tot TPM. In IT-auditingland circuleren verder diverse definities van het begrip TPM. In dit artikel wordt een TPM gezien als een schriftelijke uiting van een onafhankelijke en onpartijdige auditor

- ten behoeve van één of meer gebruikers,
- waarbij naar aanleiding van een onderzoek
- een bepaalde mate van zekerheid wordt geboden
- over het stelsel van getroffen beheermaatregelen dat de kwaliteit van de dienstverlening van een leverancier moet waarborgen.

In deze definitie is de soort dienstverlening niet van belang, maar dit artikel beperkt zich tot het uitbesteden van IT-beheeractiviteiten[2] aan een IT-serviceprovider en het uitvoeren van een TPM-onderzoek door een IT-auditor.

Voor dit artikel is een aantal gebruikersorganisaties geïnterviewd aan de hand van een vooraf opgestelde vragenlijst. De antwoorden zijn vervolgens samengevat, zodat uit het artikel niet blijkt wie wat heeft gezegd. Het betreft geen grootschalig onderzoek waarbij is getracht een representatieve deelverzameling van de gebruikersorganisaties in Nederland te interviewen. Via ons eigen persoonlijke netwerk zijn wij in contact gekomen met de geïnterviewden, waarbij wij ernaar hebben gestreefd minimaal zes gebruikersorganisaties te interviewen. Alle gebruikersorganisaties die wij hebben benaderd, waren bereid deel te nemen aan dit onderzoek.

De behoefte van gebruikersorganisaties aan een TPM zal eerst aan de orde komen. Vervolgens wordt besproken welke soorten TPM-onderzoek worden uitgevoerd, welke normenstelsels daarbij worden gebruikt en hoe het TPM-proces voor de gebruikersorganisaties verloopt. In de afsluitende beschouwingen worden ten slotte de leerpunten van het onderzoek samengevat.

1) In alfabetische volgorde worden de volgende organisaties hartelijk bedankt voor hun medewerking aan dit artikel: Akzo Nobel bv, de Belastingdienst, DAF Trucks N.V., Centrum voor Werk en Inkomen (CWI), Deutsche Bank AG, N.V. Nederlandse Gasunie, Geové RZG Zorgverzekeraar, Hoek Loos B.V. en de Rijksvoorlichtingsdienst van het Ministerie van Algemene Zaken.

2) Alhoewel een aantal geïnterviewden aangaf ook andere activiteiten te hebben uitbesteed.

Behoefte van gebruikersorganisaties aan een TPM

Een gebruikersorganisatie (klant) van een IT-serviceprovider stelt hoge eisen aan de kwaliteit van de afgesproken dienstverlening van haar IT-serviceprovider. De uitbestede IT-beheeractiviteiten, vaak ter ondersteuning van het hart van de bedrijfsvoering, zijn voor een gebruikersorganisatie een black box, waarbij alleen de output een indicatie geeft over de kwaliteit van de ontvangen dienstverlening. De meeste geïnterviewden geven aan dat zij meer zekerheid wensen omtrent het nakomen van gemaakte afspraken door de IT-serviceprovider, mede omdat daarover in sommige gevallen twijfel is ontstaan door incidenten. Zij willen dat deze zekerheid wordt gegeven door een onafhankelijke en onpartijdige instantie die de dienstverlening van de IT-serviceprovider onderzoekt. Verder geven geïnterviewden aan dat de interne accountantsdienst en/of de externe accountant[3] een oordeel van een IT-auditor eisen. Eén van de geïnterviewden geeft aan zelf geen behoefte te hebben aan een TPM en dat alleen de externe accountant het eist. Zelf heeft deze gebruikersorganisatie voldoende aan de service-levelrapportages en de gesprekken met de IT-serviceprovider. De service-levelrapportages zijn periodieke rapportages die door de IT-serviceprovider zelf zijn opgesteld naar aanleiding van de verleende diensten in een bepaalde periode. Deze rapportages dienen enerzijds ervoor de gebruikersorganisatie te laten zien of de gemaakte afspraken worden nagekomen en anderzijds als instrument voor verdere kwaliteitsverbetering. Aan de betrouwbaarheid van deze service-levelrapportages kan in een TPM-onderzoek aandacht worden geschonken.

3) De externe accountant zal alleen geïnteresseerd zijn in die aspecten van de kwaliteit van de dienstverlening door de IT-serviceprovider die van belang zijn in het kader van de jaarrekeningcontrole. De externe accountant moet in het kader van de jaarrekeningcontrole in elk geval melding maken van zijn bevindingen met betrekking tot de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking (zie vierde lid van artikel 393 van boek 2 van het Burgerlijk Wetboek). Overigens, in sommige situaties kan het voorkomen dat de interne of externe IT-auditor van een gebruikersorganisatie ook gebruik wil maken van de resultaten van een TPM-onderzoek. Denk hierbij aan de situatie dat de IT-serviceprovider zelf ook een deel van de IT-beheeractiviteiten heeft uitbesteed, waardoor een keten van uitbesteding ontstaat; de IT-serviceprovider is in deze situatie ook een gebruikersorganisatie geworden.

Gebruikersorganisaties willen doorgaans een specifieke TPM voor hun eigen situatie ontvangen.

Slechts één van de geïnterviewden geeft aan dat de behoefte aan zekerheid over de kwaliteit van de dienstverlening er wel is, maar dat het tot op heden nog niet is gelukt daarover afspraken te maken met de IT-serviceprovider. De andere organisaties krijgen inzicht in de kwaliteit van de dienstverlening door middel van een TPM, waarbij de betrokkenheid van de gebruikersorganisatie bij het TPM-onderzoek varieert van geen betrokkenheid tot en met intensieve betrokkenheid, inclusief joint-audits met de externe IT-auditor en participatie bij de afstemming van de onderzoeksresultaten; de eindverantwoordelijkheid blijft natuurlijk bij de externe IT-auditor. In de meeste gevallen is de IT-serviceprovider de opdrachtgever van de IT-auditor die het TPM-onderzoek uitvoert.

De meeste geïnterviewden geven aan een specifieke TPM voor hun eigen situatie te ontvangen en dat ook op deze manier te willen. Immers, iedere gebruikersorganisatie heeft eigen, specifieke afspraken met de IT-serviceprovider gemaakt omtrent de uitbestede IT-beheeractiviteiten. Zoals andere activiteiten, andere kwaliteit en andere service-levels. Alleen in geval van een standaarddienstverlening zou een generieke TPM toereikend kunnen zijn, bijvoorbeeld voor de uitbesteding van een personeelssysteem. Maar ook hier kan de afhankelijkheid van zo'n systeem per gebruikersorganisatie verschillen en kunnen andere eisen aan de kwaliteit van de dienstverlening worden gesteld. Voor een aantal geïnterviewden zou het ook acceptabel zijn indien een generieke TPM wordt ontvangen en daarnaast voor specifieke zaken een aparte TPM.

De geïnterviewden betalen de kosten van het jaarlijkse TPM-onderzoek in de meeste gevallen zelf, al dan niet via de IT-serviceprovider; indirect betalen de gebruikersorganisaties deze kosten natuurlijk altijd zelf. In één geval worden de kosten van de TPM bekostigd door de IT-serviceprovider en gebruikersorganisatie en uit het jaarrekeningcontrolebudget van de externe accountant. Een aantal geïnterviewden geeft aan dat de hoge kosten van een TPM-onderzoek wel tot discussie met de IT-serviceprovider hebben geleid:

- Wie moet de kosten van het TPM-onderzoek betalen?
- In hoeverre mag de IT-serviceprovider ter vergoeding van de eigen urenbesteding voor de medewerking aan het TPM-onderzoek een opslag op de rekening van de IT-auditor aan de gebruikersorganisatie doorberekenen?
- Is de kosten-batenverhouding van een TPM gunstig?

Soorten TPM-onderzoek

Internationaal en nationaal zijn er op auditgebied belangwekkende ontwikkelingen geweest, zoals het auditframework *International Standard on Auditing 100* van de International Federation of Accountants ([IFAC00]) en de *IS Auditing Guideline Reporting 070.010* van de Information Systems Audit and Control Association & Foundation ([ISAC03]). Definities en te hanteren bewoordingen zijn hierdoor verder aangescherpt. In essentie worden drie soorten TPM-onderzoek onderkend (zie ook elders in deze Compact het artikel van Van Langen), te weten:

- *Overeengekomen Specifieke Werkzaamheden (OSW)*, waarbij de opdrachtgever een beslissende invloed heeft op de aard en diepgang van de door de auditor te verrichten werkzaamheden; de overeengekomen werkzaamheden kunnen natuurlijk bestaan uit het toetsen aan normen. De auditor kan en mag in geval van een OSW geen oordeel of conclusie geven omtrent het stelsel van getroffen beheermaatregelen dat de kwaliteit van de dienstverlening van een IT-serviceprovider moet waarborgen en mag alleen de feitelijke bevindingen rapporteren. De IT-auditor geeft dus alleen zekerheid omtrent de bevindingen en geen zekerheid omtrent het stelsel van getroffen beheermaatregelen. De gebruiker van het rapport moet zelf zijn/haar conclusie op basis van het rapport van de auditor vormen. Een OSW betreft dus geen assuranceopdracht.
- *Review*, waarbij de IT-auditor toetst aan normen en een beperkte mate van zekerheid[4] kan geven omtrent het stelsel van getroffen beheermaatregelen dat de kwaliteit van de dienstverlening van een IT-serviceprovider moet waarborgen. Dit betreft dus een assuranceopdracht.
- *Audit*, waarbij de IT-auditor toetst aan normen en een redelijke mate van zekerheid[5] kan geven omtrent het stelsel van getroffen beheermaatregelen dat de kwaliteit

4) 'Limited assurance' in het Engels.

5) 'Reasonable assurance' in het Engels.

van de dienstverlening van een IT-serviceprovider moet waarborgen. Dit betreft dus ook een assuranceopdracht.

De geïnterviewden geven aan dat het ten behoeve van hun organisatie uitgevoerde TPM-onderzoek een review of audit betreft, dus te classificeren als een assuranceopdracht. Bij bestudering van de betrokken TPM'en bleek echter dat telkens een redelijke mate van zekerheid was gegeven omtrent het stelsel van getroffen beheermaatregelen dat de kwaliteit van de dienstverlening van een IT-serviceprovider moet waarborgen. Uitgaande van de huidige vaktechnische richtlijnen zal de term review moeten worden vervangen door audit of zal de mate van zekerheid die naar aanleiding van de review kan worden gegeven, worden teruggebracht tot 'beperkte mate van zekerheid'.

Specifiek of generiek normenstelsel

Alle third-partymededelingen die de geïnterviewden tot nu toe hebben ontvangen, waren het resultaat van het toetsen aan normen. Op de vraag in hoeverre de gebruikersorganisatie invloed heeft gehad op het gehanteerde normenstelsel, geven de meeste geïnterviewden aan dat zij dat wel hebben gehad. Meestal is een door de IT-auditor beschikbaar gesteld normenstelsel samen met de IT-serviceprovider en de auditor aangepast aan de specifieke situatie en vervolgens gezamenlijk vastgesteld. De meeste gebruikersorganisaties geven aan dat het vastgestelde normenstelsel in de praktijk voldoet. Een enkeling geeft aan dat het normenstelsel achteraf toch niet toereikend bleek, omdat de gebruikersorganisatie – nadat de TPM was uitgebracht – toch nog met vragen bleef zitten.

Tegenwoordig is een aantal internationaal bekende normenstelsels beschikbaar. Denk hierbij aan de BS 7799 (Code voor Informatiebeveiliging), CobIT en SysTrust. Echter, geen van deze normenstelsels wordt in brede kring erkend door gebruikersorganisaties, IT-serviceproviders en IT-auditors om er de dienstverlening van de IT-serviceprovider aan te toetsen. De mening van de geïnterviewden ten aanzien van de toereikendheid van een generiek normenstelsel geeft een verdeeld beeld te zien. De voorstanders geven als redenen aan dat er in geval van een generiek normenstelsel geen ontwikkelingskosten voor het normenstelsel hoeven te worden gemaakt en dat een generiek normenstelsel de objectiviteit van de TPM bevordert. Tegenstanders geven aan dat een generiek normenstelsel te beperkt of te veeleisend voor de specifieke situatie kan zijn en dat het daardoor altijd noodzakelijk is het generieke normenstelsel op maat te maken voor de specifieke situatie. Denk hierbij aan verschillen als gevolg van de branche van de gebruikersorganisatie, het uitbestede platform, etc.

TPM-proces

Op één na gaven de geïnterviewden aan dat het TPM-onderzoek jaarlijks wordt uitgevoerd en dat zij naar aanleiding daarvan een TPM ontvangen of mogen inzien bij de IT-serviceprovider. Eén van de geïnterviewden gaf aan dat – in overleg met de externe accountant – vanaf heden het TPM-onderzoek niet meer automatisch jaarlijks zal worden uitgevoerd, maar slechts op verzoek van de gebruikersorganisatie. Dit in verband met de hoge kosten voor rekening van de gebruikersorganisatie en vanwege het feit dat op andere manieren ook inzicht kan worden verkregen in de kwaliteit van de dienstverlening door de IT-serviceprovider, zoals een ISO-certificaat en communicatie over het doorvoeren van changes.

Bij de keuze van een IT-auditor eisen gebruikersorganisaties doorgaans een IT-auditorganisatie van naam en faam.

De meeste geïnterviewden gaven aan dat de TPM in hun situatie voldoet aan hetgeen zij ervan verwachten, waarbij één van de geïnterviewden aangaf dat naast de TPM ook eigen audits inzicht gaven in de kwaliteit van de dienstverlening door de IT-serviceprovider. De reikwijdte betreft meestal 'opzet[6] en bestaan[7]' of 'opzet en werking[8]'. In de gevallen dat de geïnterviewde niet helemaal tevreden was, werd als reden aangevoerd dat de TPM beperkt was tot opzet en bestaan van de IT-beheermaatregelen, terwijl ook de behoefte bestond om inzicht te krijgen in de werking ervan. Ook werd een te beperkt geheel van onderzoeksobjecten als reden genoemd, zoals onderzoek van slechts de generieke dienstverlening of een gedeelte van de uitbestede IT-beheeractiviteiten.

De meeste geïnterviewden gaven aan dat een IT-auditorganisatie van naam en faam een eis is bij de keuze van de IT-auditor. Verder gaven zij aan geen invloed te hebben gehad op de keuze van de IT-auditor, maar omdat het een IT-auditor was van één van de grote accountantskantoren, was dit geen probleem. Sommige geïnterviewden opperden dat een ingehuurde interne IT-auditor van een (internationale) organisatie van naam en faam het generieke onderzoek ook zou kunnen uitvoeren, zolang de deskundigheid (RE met verstand van techniek), onpartijdigheid en onafhankelijkheid in voldoende mate zouden zijn gewaarborgd. Echter, de externe accountant van de gebruikersorganisatie die belast is met de controle van de jaarrekening mag volgens de Richtlijnen voor de Accountantscontrole (RAC) geen controlebewijs ontlenen aan een TPM afgegeven door een dergelijke IT-auditor. Zie hiervoor de richtlijnen 402 en 620 uit de RAC 2002. Richtlijn 402 'Overwegingen bij controles van huishoudingen die gebruikmaken van service-organisaties' is hier van toepassing. Dit vanwege het feit dat de TPM van de ingehuurde interne IT-auditor van een andere organisatie geen rapport voor derden betreft dat is uitgebracht door de externe accountant van de serviceorganisatie, interne accountant of toezichthouder. Richtlijn 620 'Gebruikmaken van de werkzaamheden van deskundigen' is hier niet van toepassing, omdat de ingehuurde interne IT-auditor niet in dienst is van de gebruikersorganisatie of haar externe accountant. De externe accountant dient in deze situatie alsnog zelf onderzoek te doen bij de IT-serviceprovider, waarbij de TPM – inclusief een uitgebreide rapportage van bevindingen – van deze ingehuurde interne IT-auditor wel als informatiebron kan worden gebruikt.

6) 'Opzet' heeft betrekking op het voldoen aan de normen van het stelsel van beheermaatregelen dat zou moeten zijn/worden geïmplementeerd (adequaat ontwerp van het voorgeschreven stelsel van beheermaatregelen).

7) 'Bestaan' heeft betrekking op de feitelijke toepassing van het voorgeschreven stelsel van beheermaatregelen op een bepaald moment (effectieve implementatie).

8) 'Werking' heeft betrekking op de feitelijke toepassing van het voorgeschreven stelsel van beheermaatregelen gedurende een bepaalde periode (effectieve uitvoering).

Een andere mogelijkheid die werd geopperd, is een joint-audit door de IAD van de gebruikersorganisatie en die van de IT-serviceprovider, maar dit zal voor een IT-serviceprovider met meerdere klanten veel werk opleveren.

Het TPM-onderzoek wordt over het algemeen uitgevoerd buiten het zicht van de gebruikersorganisatie. De helft van de geïnterviewden wordt niet op de hoogte gehouden omtrent het verloop van het TPM-onderzoek en de tussenresultaten (de meesten van hen zijn overigens geen opdrachtgever). Afgezien van de formulering van de TPM-onderzoeksopdracht (normenstelsel, reikwijdte, diepgang, timing, etc.) wordt alleen het resultaat ervan bekendgemaakt aan de gebruikersorganisatie. Andere gebruikersorganisaties worden wel tussentijds op de hoogte gehouden door middel van periodiek overleg, voortgangsbesprekingen en/of tussenrapportages, of mogen zelfs een bijdrage leveren aan de onderzoeken (joint-audit). De geïnterviewden die invloed willen op het TPM-proces geven aan dat in voldoende mate te hebben.

Vanuit de gebruikersorganisaties gezien is verbetering van het TPM-proces nog mogelijk op het gebied van:
- planning en voortgang van het TPM-onderzoek;
- door de IT-auditor uit te voeren werkzaamheden;
- onderbouwing van conclusies; en
- opvolging van negatieve bevindingen.

De meeste geïnterviewden geven aan dat de negatieve bevindingen uit de TPM-rapportage goed en in overleg met de gebruikersorganisatie worden opgepakt door de IT-serviceprovider. Volgens hen heeft de IT-auditor hierin in principe geen rol.

Voor de geïnterviewden bevat de ideale TPM de volledige rapportage van de IT-auditor (mededeling, normenstelsel en detailbevindingen), aangevuld met de gerealiseerde verbeteringen ten opzichte van de vorige TPM.

Afsluitende beschouwing

Uit het onderzoek is gebleken dat het begrip TPM leeft onder gebruikersorganisaties. Wel is duidelijk geworden dat op het gebied van eenduidigheid nog het een en ander te doen is in IT-auditingland, zoals met betrekking tot definities, mate van zekerheid, wijze van rapportage en te hanteren bewoordingen.

> In de meeste gevallen heeft een TPM een positieve invloed gehad op de kwaliteit van de dienstverlening van de IT-serviceprovider.

De geïnterviewden zijn over het algemeen positief over TPM'en. Bovendien zijn zij over het algemeen ook positief over hun IT-serviceprovider. Wellicht dat de openheid van zaken die de IT-serviceprovider met een TPM geeft, het vertrouwen in en de goede relatie met de IT-serviceprovider bevordert.

De meeste geïnterviewden geven aan dat een TPM een positieve invloed heeft gehad op de kwaliteit van de dienstverlening van de IT-serviceprovider. Het gevoel van de geïnterviewden was dat het de IT-serviceprovider scherp houdt en dat het leidt tot betere procedures bij zowel de IT-serviceprovider als de gebruikersorganisatie en tot betere afstemming tussen de IT-serviceprovider en de gebruikersorganisatie.

Duidelijk is ook de voorkeur voor een specifieke TPM voor de eigen situatie, omdat iedere gebruikersorganisatie uniek is (in elk geval hebben veel gebruikersorganisaties dat gevoel). Uit oogpunt van efficiëntie is een generieke TPM, aangevuld met een specifieke TPM voor iedere gebruikersorganisatie die daarom vraagt, voor zowel de gebruikersorganisaties als hun IT-serviceprovider te prefereren.

Voor de duidelijkheid voor zowel de gebruikersorganisatie, IT-serviceprovider als de IT-auditor is het wellicht zinvol uit te gaan van een generiek normenstelsel en in de TPM duidelijk aan te geven welke normen niet van toepassing zijn (en waarom) en welke normen zijn toegevoegd voor de specifieke situatie. Hierdoor ontstaat in elk geval een voor iedereen duidelijk referentiekader. Op dit moment is de ene TPM de andere niet, met name doordat de gehanteerde normenstelsels onderling grote verschillen vertonen, waardoor het risico bestaat dat de verwachting van een (potentiële) gebruikersorganisatie niet wordt waargemaakt. Indien de IT-serviceprovider met zijn klanten zoveel mogelijk dezelfde afspraken maakt, dan bevordert dit de efficiëntie van het TPM-onderzoek. Dit kan natuurlijk haaks staan op de commerciële afwegingen van de IT-serviceprovider.

Op één na geven alle geïnterviewden aan te zullen doorgaan met de jaarlijkse TPM-onderzoeken bij de IT-serviceprovider. Sommige zien het als een essentiële voorwaarde bij outsourcingtrajecten, waarbij natuurlijk vóór ondertekening van het uitbestedingscontract duidelijke afspraken moeten worden gemaakt over de aanpak en kosten van het TPM-onderzoek. De geïnterviewde die heeft aangegeven niet verder te willen gaan met het jaarlijkse TPM-onderzoek, geeft aan dat alleen de externe accountant behoefte heeft aan een TPM; de gebruikersorganisatie zelf heeft voldoende aan de service-levelrapportages van en de gesprekken met de IT-serviceprovider zelf. Voorwaarde hierbij is natuurlijk een zeer goede verstandhouding met de IT-serviceprovider en volledig vertrouwen van de gebruikersorganisatie in de IT-serviceprovider.

Gezien de steeds groter wordende afhankelijkheid van uitbestede IT-beheeractiviteiten is aan de geïnterviewden gevraagd in hoeverre een wettelijke plicht inzake een TPM aan de orde is (vergelijk de accountantsverklaring bij een jaarrekening). Hierop is verdeeld gereageerd. De tegenstanders geven onder andere aan dat dit vooralsnog te ver gaat en dat IT-serviceproviders zich gewoon aan de afspraken moeten houden; wellicht dat het voor bepaalde branches wel verplicht zou moeten zijn, zoals de bankensector. De voorstanders voeren aan dat een

TPM inzicht geeft in de black box die de IT-beheeractiviteiten na uitbesteding zijn geworden en dat het vertrouwen in de IT-serviceprovider wordt vergroot. Bovendien blijf je als uitbestedende organisatie altijd eindverantwoordelijk voor je eigen bedrijfsproces, ook al zijn delen daarvan uitbesteed. Daarnaast menen zij dat het discussies kan voorkomen die gebruikersorganisaties en IT-serviceproviders kunnen hebben bij het komen tot een TPM-onderzoek, zoals:

- Welke mate van zekerheid over het getroffen stelsel van beheermaatregelen is nodig?
- Welke toetsingsnormen te hanteren?
- Welke auditstandaarden[9] te hanteren?
- Welke kwaliteitsaspecten te onderzoeken?
- Welke reikwijdte (scope)?
- Welke onderzoeksobjecten?
- Welke inhoud hebben de TPM-rapportages?
- Wie is de opdrachtgever voor de IT-auditor?
- Op welke wijze worden de kosten van het TPM-onderzoek verrekend tussen de IT-serviceprovider en de gebruikersorganisatie?
- Wat houden de kosten van het TPM-onderzoek in? Alleen de declaratie van de IT-auditor?

Een deskundige en gekwalificeerde IT-auditor kan hierbij een begeleidende en adviserende rol spelen. En zoals één van de geïnterviewden aangaf: vertrouwen in je IT-serviceprovider is goed, controle is beter en aantonen met een TPM van een onafhankelijke en onpartijdige IT-auditor is het beste.

Literatuur

[IFAC00]
International Federation of Accountants (IFAC), *International Standard on Auditing (ISA) 100, Assurance Engagements*, juni 2000.

[ISAC03]
Information Systems Audit and Control Association & Foundation (ISACA), *IS Auditing Guideline Reporting 070.010*, oktober 2002.

9) Afhankelijk van de (combinatie van) beroepskwalificatie(s), zoals Register EDP-Auditor (RE), Certified Information Systems Auditor (CISA) en Register Accountant (RA), en de behoefte van de klant zal voor de uitvoering van een TPM-onderzoek een auditstandaard worden gehanteerd. De keuze voor een bepaalde auditstandaard kan consequenties hebben voor de keuze van het te hanteren normenstelsel, de aanpak van het onderzoek, het gebruik van een managementbewering en de wijze van rapporteren.

Mw. drs. S. van der Eijk-van Eck
is werkzaam bij KPMG Information Risk Management en is de afgelopen jaren betrokken geweest bij diverse third-party-audits op het gebied van beheer van rekencentra.

vandereijk.silvie@kpmg.nl

Drs. K.H.G.J.M. Ho RE RA
is werkzaam als senior manager bij KPMG Information Risk Management. Hij heeft zich de afgelopen jaren primair beziggehouden met advisering en auditing op het gebied van planning en beheersing van IT-projecten, kwaliteit van systeemontwikkeling en beheer van rekencentra. Daarnaast houdt de heer Ho zich bezig met het verder ontwikkelen van de IRM-dienstverlening die leidt tot third-party-mededelingen. Verder is hij als vaktechnisch coördinator betrokken bij de postdoctorale EDP-Audit Opleiding van de Vrije Universiteit te Amsterdam.

ho.kaihang@kpmg.nl