Professioneel kader van de TPM-opdracht

Drs. R.J.M van Langen RE RA

De uitkomsten van de werkzaamheden van een IT-auditor hoeven niet alleen bestemd te zijn voor de opdrachtgever. Steeds vaker worden uitingen van een IT-auditor in de openbaarheid gebracht. Voorbeelden hiervan zijn: ZekeRE Business, ZekeRE Privacy, SAS 70-rapportages, WebTrustzegels of een certificaat bij een softwarepakket. De wijze waarop dergelijke uitkomsten aan het maatschappelijk verkeer worden geuit, verschillen in detaillering en omvang (van een simpel zegel/keurmerk tot aan een omvangrijke rapportage), maar ook de doelgroep, diepgang en andere aspecten van dergelijke opdrachten kunnen wezenlijk van elkaar verschillen. In dit artikel worden de diverse aspecten van een TPM-opdracht nader belicht.

Inleiding

Bij uitbesteding van automatiseringsdiensten worden de automatiseringstaken uitgevoerd door een IT-service-provider. De uitbestedende organisatie is en blijft echter wel verantwoordelijk voor een adequate gegevensverwerking. Enerzijds zal de uitbestedende organisatie haar eisen definiëren in bijvoorbeeld een service level agreement, anderzijds verlangt zij ook enige zekerheid dat de dienstverlening van de IT-serviceprovider voldoet aan de gestelde eisen. Die zekerheid kan door een IT-auditor worden gegeven in de vorm van een third-partymededeling (TPM).
Ook bij het verrichten van elektronische transacties kan een gebruiker zekerheid wensen omtrent bijvoorbeeld de getroffen beveiligingsmaatregelen ten behoeve van het waarborgen van een betrouwbare afhandeling van de transactie. De mate van zekerheid die wordt verschaft, hangt af van het uitgevoerde onderzoek en de aard van het onderzoeksobject en de daarmee samenhangende kwantiteit en kwaliteit van het beschikbare bewijsmateriaal.

In dit artikel over het professionele kader van de TPM-opdracht wordt eerst een definitie gegeven van een TPM-opdracht. Vervolgens komen de diverse aspecten van een TPM-opdracht aan bod. Deze aspecten zijn onder meer de te onderkennen gebruikersgroepen, de mate van zekerheid en reikwijdte van een TPM-opdracht, aandachtspunten bij de uitvoering en de rapportagevorm. Naast de te onderscheiden kenmerken wordt, indien relevant, nadere uitwerking gegeven aan deze aspecten bij de diverse vormen van TPM-opdrachten.

Bij het onderkennen van de verschillende aspecten is aansluiting gezocht bij het raamwerk van assurance-opdrachten. Dit raamwerk is door de International Federation of Accountants (IFAC) medio 2000 gepubliceerd (ISA100 ([IFAC02])). In 2003 heeft IFAC een Exposure Draft gepubliceerd met als titel *Proposed 'International Framework For Assurance Engagements', Proposed ISAE 2000 'Assurance Engagements On Subject Matters Other Than Historical Financial Information' and Proposed Withdrawal of ISA 120 'Framework of International Standards on Auditing', to Replace International Standard on Assurance Engagements 100, Assurance Engagements* ([IFAC03]). Deze Exposure Draft geeft naast een herziening van ISA100 tevens een raamwerk (ISAE2000) voor assuranceopdrachten voor andere objecten dan historische financiële informatie (zoals een jaarrekening). Deze Exposure Draft biedt daarmee veel aanknopingspunten voor de diverse aspecten van een TPM-opdracht.

Definitie van een TPM-opdracht

Een eenduidige definitie van een TPM-opdracht is niet beschikbaar. In het *Handboek EDP-auditing* ([NIVR01a]) wordt wel de term TPM genoemd, maar hierbij is geen definitie vermeld.
Veltman vermeldt in zijn artikel ([Velt95]) dat een TPM een schriftelijke mededeling betreft van een service-auditor inhoudende de uitkomst van een onderzoek naar de interne controle bij een serviceorganisatie, ten behoeve van één of meer derden.
In [Keij02] wordt een TPM gedefinieerd als third party assurance, onafhankelijke assurance met betrekking tot de interne beheersing van processen ten behoeve van (een groot aantal) externe partijen die niet altijd vooraf bij naam bekend zijn.

Alvorens te komen tot een eigen definitie zal eerst worden ingegaan op de te onderkennen partijen en aard van een TPM-opdracht.

Partijen bij een TPM-opdracht

Naar analogie van de *International Framework For Assurance Engagements* ([IFAC03]) kunnen de volgende drie partijen worden onderscheiden:
- de verantwoordelijke partij;
- de beoogde gebruiker; en
- de beroepsbeoefenaar.

De *verantwoordelijke partij* is de persoon (of de groep personen) die, als individu of als vertegenwoordigers van een huishouding, verantwoordelijk is (zijn) voor (het functioneren van) het object van onderzoek.

De *beoogde gebruiker* is de persoon of de groep personen voor wie de beroepsbeoefenaar zijn TPM (voor een specifiek gebruiksdoel) opstelt. De verantwoordelijke partij kan zelf één van de beoogde gebruikers zijn, maar niet de enige. De verantwoordelijke partij en de beoogde gebruiker zijn vaak afkomstig uit verschillende organisaties. Dit is echter niet altijd het geval; zo kan de leiding van een concernonderdeel zekerheid wensen te verkrijgen over bijvoorbeeld het centrale rekencentrum binnen het concern waar een ander verantwoordelijk voor is. De relatie tussen de verantwoordelijke partij en de beoogde gebruiker dient te worden gezien in de context van de opdracht.

De *beroepsbeoefenaar* is de opdrachtnemer die de TPM afgeeft en is in de herziene ISA100 ([IFAC03]) gedefinieerd als de (openbare) accountant die verbonden is aan een organisatie die lid is van IFAC. In dit artikel wordt echter de onafhankelijke IT-auditor als de beroepsbeoefenaar beschouwd.

Bij een third-partymededeling worden, zoals de term aangeeft, de uitkomsten van het onderzoek gerapporteerd aan een derde. De term 'third party' heeft in dit verband betrekking op de beoogde gebruiker, die als derde partij een mededeling verlangt. Vanuit de optiek van de beoogde gebruiker en verantwoordelijke partij wordt de beroepsbeoefenaar als (onafhankelijke) derde in het kader van de TPM gezien.

Een opdracht voor het verrichten van overeengekomen specifieke werkzaamheden kan onder bepaalde condities een TPM-opdracht zijn.

Een partij die hierboven niet is benoemd, is de opdrachtgever van de TPM-opdracht. Indien de beoogde gebruiker de opdrachtgever is, dan wordt niet *aan* een derde maar *over* een derde gerapporteerd. In de praktijk wordt een dergelijke opdracht echter ook gezien als een TPM-opdracht. Maar de afstemming van de opdrachtformulering met de beoogde gebruiker alsmede de wijze waarop de uitkomsten van het onderzoek worden gerapporteerd, zullen door de opdrachtgever worden bepaald. Hierdoor kan afhankelijk van wie de opdrachtgever is, de opdracht(omschrijving) een verschillende inhoud hebben.

Aard van een TPM-opdracht

In de herziene ISA100 ([IFAC03]) is onderkend dat naast assuranceopdrachten ook andersoortige opdrachten bestaan, zoals opdrachten tot het verrichten van overeengekomen specifieke werkzaamheden. De vraag is dan ook of een TPM-opdracht uitsluitend een assuranceopdracht is, of dat een TPM-opdracht ook in de vorm van het verrichten van overeengekomen specifieke werkzaamheden kan worden uitgevoerd.

In RAC920 ([NIVR02]) is aangegeven dat de uitkomsten van een dergelijk onderzoek aan meerdere partijen kunnen worden gerapporteerd. Paragraaf 6 van RAC920 vermeldt namelijk 'Het rapport is uitsluitend bestemd voor partijen waarmee de te verrichten werkzaamheden zijn overeengekomen', waarmee de mogelijkheid van meerdere partijen is onderkend.

Daarnaast is in Audit Alert 11 ([NIVR01]) aangegeven dat de toetsing en beoordeling op hoofdlijnen ter zake van de toereikendheid van de organisatie-inrichting en het beheersingsmechanisme door de externe accountant in het kader van de ROB (Regeling Organisatie en Beheer) van De Nederlandsche Bank een vorm is van een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden.

In de Amerikaanse SSAE10 (AT Section 101 van [AICP02]) omvat een Attestation Engagement 'an examination, a review, or an agreed-upon procedures report on subject matter, or an assertion about the subject matter, that is the responsibility of another party'. Een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden wordt dus ook tot Attestation Engagement gerekend.

ISACA tot slot vermeldt in haar rapportagerichtlijn ([ISAC02]) dat een opdracht tot het rapporteren over de effectiviteit van beheersingsmaatregelen kan worden uitgevoerd door middel van de volgende soorten van assuranceservices:
- audit;
- review;
- agreed-upon procedures.

ISACA definieert derhalve een assuranceopdracht breder dan IFAC in de herziene ISA100 ([IFAC03]), waar een 'agreed-upon procedures'-opdracht niet tot een assuranceopdracht wordt gerekend. In dit artikel wordt voor de term assuranceopdracht de definitie gehanteerd uit de *International Framework For Assurance Engagements*.

Een opdracht voor het verrichten van overeengekomen specifieke werkzaamheden kan ook leiden tot een mededeling aan een derde en is daarom een vorm van een TPM-opdracht.

Een TPM-opdracht wordt in dit artikel als volgt gedefinieerd:
Een TPM-opdracht is een assuranceopdracht of een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden (OSW) waarbij de gebruiker van de TPM niet tot dezelfde organisatie behoort als de verantwoordelijke partij voor het onderzoeksobject, of daartoe op vergelijkbare afstand staat (in concernverband).

De mate van zekerheid van een TPM-opdracht is voor een OSW-opdracht anders dan bij een assuranceopdracht. In de volgende paragraaf worden dit en andere aspecten van een TPM-opdracht nader uiteengezet.

Aspecten van een TPM-opdracht

Bij TPM-opdrachten kunnen de gehanteerde normen en het onderzoeksobject van elkaar verschillen. Een eenduidige opdrachtomschrijving en rapportering is daarom

van belang. Daarbij is het belangrijk dat geen grotere verwachtingen worden gewekt dan kunnen worden waargemaakt.

Gebruikersgroepen

Bij TPM-opdrachten kunnen de volgende gebruikersgroepen, naar analogie van NOREA ([NORE02]) worden onderscheiden:
* één bekende gebruiker of een beperkte kring van bekende gebruikers (een specifieke doelgroep);
* (deels) onbekende gebruikers (maatschappelijk verkeer).

NOREA onderscheidt daarnaast nog de opdrachtgever als mogelijke doelgroep. Indien de opdrachtgever één van de beoogde gebruikers is, dan valt dit onder de categorie specifieke doelgroep. Zoals hiervoor bij 'Partijen bij een TPM-opdracht' is vermeld, kan afhankelijk van wie de opdrachtgever is, de opdracht(omschrijving) een verschillende inhoud hebben. Daarnaast wordt nog opgemerkt dat indien de opdrachtgever de enige gebruiker en tevens de verantwoordelijke partij is, er dan geen sprake meer is van een TPM-opdracht (hetgeen in overeenstemming is met de herziene ISA100 en SSAE10 en ook in de hiervoor vermelde definitie is opgenomen).

Het onderkennen van de gebruikersgroep is relevant voor het bepalen van de TPM-opdracht (en haar elementen) en de wijze van de rapportering. 'De IT-auditor zal bij het bepalen van de inhoud en woordkeus van de rapportage uitgaan van een minimum kennis- en ervaringsniveau van de doelgroep' ([NORE02]). De gebruikersgroep is derhalve van belang voor een aantal van de hierna behandelde aspecten.

Mate van zekerheid

Een TPM-opdracht is een assuranceopdracht of een OSW-opdracht. De NOREA heeft in haar richtlijnen (in het kader van de attestfunctie) deze typen van opdrachten nog niet gedefinieerd en/of gehanteerd. In het *Jaarboek 2003* ([NORE03]) is aangekondigd dat het bestuur heeft besloten aansluiting te zoeken met internationaal erkende regelgeving voor auditors. Een ontwerp van de 'NOREA-Code of Ethics' wordt gebaseerd op de 'Code of Ethics' van IFAC ([IFAC01]). In de 'Code of Ethics' van IFAC is in de paragrafen 8.3 tot en met 8.6 de aard van assuranceopdrachten (conform ISA100) beschreven en tevens is hierin vermeld de opdracht 'tot het verrichten van overeengekomen specifieke werkzaamheden' als vorm van een niet-assuranceopdracht. Het hanteren van de term assuranceopdracht wordt in dat licht dan ook mogelijk gangbaar voor IT-auditopdrachten in Nederland.

Assuranceopdracht
Een TPM-opdracht als assuranceopdracht is een audit of een review, die is gericht op het verkrijgen van een redelijke respectievelijk beperkte mate van zekerheid omtrent een onderzoeksobject op basis van criteria.
De termen 'audit' en 'review' en 'mate van zekerheid' zijn in kader 1 respectievelijk 2 (volgende pagina) nader toegelicht.

De termen 'audit' en 'review'
De term 'audit' wordt soms één op één geassocieerd met de controle van een jaarrekening. In [FEDE03] van de Europese Accountantsorganisatie FEE is zelfs bepleit om de termen 'audit' en 'review' alleen te gebruiken in het kader van de controle respectievelijk beoordeling van een jaarrekening. Voor andersoortige opdrachten worden de termen 'Examination' en 'Survey' als suggestie genoemd. In ISAE2000 ([IFAC03]), die ingaat op assuranceopdrachten voor onderzoeksobjecten anders dan de historische financiële informatie, worden echter ook de termen 'audit-level' en 'review-level' gehanteerd. Hierbij is wel aangegeven dat ook synoniemen als 'examination' respectievelijk 'limited review' worden gehanteerd.
ISACA heeft in [ISAC02] de termen 'audit' en 'review' geadopteerd in haar definitie van assurance services voor het rapporteren over de effectiviteit van beheersingsmaatregelen.
De termen 'audit' en 'review' of 'IT-audit' en 'IT-review' zijn daarom geëigende termen voor een TPM-opdracht als assuranceopdracht, maar zijn nog zeker geen algemeen aanvaarde begrippen binnen het vakgebied van IT-auditing en het maatschappelijk verkeer.

Kader 1. De termen 'audit' en 'review'.

De termen 'audit' en 'review' zijn geen eenduidig gedefinieerde begrippen binnen het vakgebied van IT-auditing, laat staan het maatschappelijk verkeer (zie ook kader 1). Vooral bij een review bestaat het risico dat de gebruiker zich onvoldoende bewust is van de beperkte mate van zekerheid die deze biedt (zie ook kader 2).

Een TPM-opdracht in de vorm van een reviewopdracht lijkt dan ook alleen aanvaardbaar indien er sprake is van één bekende gebruiker of een beperkte kring van bekende gebruikers waarbij de betekenis van de diepgang van de opdracht bij de beoogde gebruikers bekend mag worden verondersteld. Dit met name om te voorkomen dat een verwachtingskloof ontstaat door een verkeerde interpretatie van de werkzaamheden en rapportage van de IT-auditor.

Het onderkennen van de gebruikersgroep is relevant voor het bepalen van de TPM-opdracht.

Daarnaast wordt nog opgemerkt dat het gebruikelijk is dat een reviewopdracht die gericht is op het verkrijgen van een beperkte mate van zekerheid leidt tot een negatief geformuleerde conclusie (met de bewoordingen: 'op basis van de werkzaamheden is ons niets gebleken op basis waarvan wij zouden moeten concluderen dat het onderzoeksobject niet voldoet aan de gestelde criteria').

OSW-opdracht
Bij een opdracht tot overeengekomen specifieke werkzaamheden (OSW) rapporteert de IT-auditor slechts over de feitelijke bevindingen waardoor geen zekerheid tot uitdrukking wordt gebracht anders dan ter zake van de aspecten welke zijn onderzocht en waarover dienovereenkomstig wordt gerapporteerd. Een OSW-opdracht leidt tot een rapport van bevindingen waarin geen conclusie of oordeel wordt vermeld. In plaats daarvan beoordelen de gebruikers van de mededeling zelf de door de IT-auditor dienovereenkomstig gerapporteerde

Het begrip 'mate van zekerheid'
In RAC 120 ([NIVR02]) is vermeld dat: 'Bij een controleopdracht verschaft de accountant een (relatief) hoge maar niet absolute mate van zekerheid dat de gecontroleerde informatie geen onjuistheden van materieel belang bevat. Dit wordt in de verklaring in positief geformuleerde bewoordingen als 'redelijke mate van zekerheid' verwoord.' De termen 'hoge mate van zekerheid' en 'redelijke mate van zekerheid' worden beide gehanteerd in deze definitie.
In de herziene ISA100 ([IFAC03]) wordt de term 'high assurance' niet meer gehanteerd en wordt uitsluitend nog gesproken van 'reasonable assurance' naast 'limited assurance'. Ook in [FEDE03] is beargumenteerd om 'hoge mate van zekerheid' niet meer te hanteren.

'Reasonable assurance' omvat volgens [FEDE03] (paragraaf 151) op een schaal van nul tot honderd procent het gebied tussen 'greater than the balance of the probabilities (50%), usually less than virtual certainty but always less than absolute assurance (100%)'. De term 'limited assurance' of beperkte mate van zekerheid is in [FEDE03] niet afgezet op een schaal van nul tot honderd procent, maar hierbij is aangegeven dat 'Limited means no more than less than what could otherwise reasonably have been obtained' ([FEDE03], paragraaf 152). Eerder is vermeld 'Furthermore, practitioners tend to view moderate assurance as representing an absolute concept that is clearly below high and tends not to fall below 50%, the balance of the probabilities' maar ook 'limited assurance simply ranks lower than reasonable assurance due to the decision to obtain less evidence' ([FEDE03], paragraaf 48 respectievelijk 53).

In een studie van de International Auditing and Assurance Standards Board ([IFAC02]) zijn andere percentages genoemd voor 'Percentage of Confidence of Moderate versus High Level of Assurance'. De percentages zijn op basis van een internationale enquête onder accountantskantoren berekend. Voor een opdracht die leidt tot een beperkte mate van zekerheid is een gemiddelde berekend van 60 procent, met een (grote) bandbreedte variërend van 10 tot 88 procent. Voor een opdracht die leidt tot een hoge mate van zekerheid is een gemiddelde genoemd van 88 procent met een bandbreedte variërend van 55 tot 98 procent.

Hoewel de termen 'redelijke mate van zekerheid' en 'beperkte mate van zekerheid' relatieve begrippen zijn, geeft een zone op een schaal van nul tot honderd wel een eenduidiger betekenis. Zeker als in dit verband een beperkte mate van zekerheid wordt vereenzelvigd met minder dan 50 procent zekerheid! Het voert in het kader van dit artikel te ver om het zekerheidsconcept verder uit te werken.

Kader 2. Het begrip 'mate van zekerheid'.

werkzaamheden en bevindingen en trekken hun eigen conclusies uit het werk van de IT-auditor.

Een TPM-opdracht waarbij overeengekomen specifieke werkzaamheden worden uitgevoerd, is overeenkomstig algemeen aanvaarde standaarden alleen toegestaan indien de beoogde gebruikers betrokken zijn geweest bij de opdrachtformulering. Andere gebruikers die niet op de hoogte zijn van het doel en de aard van de werkzaamheden kunnen de uitkomsten van een dergelijke TPM-opdracht verkeerd interpreteren.

Criteria

De term criteria refereert aan de gehanteerde normen. In het kader van een TPM-opdracht zullen deze criteria
* of bekend en toegankelijk moeten zijn (bijvoorbeeld aan de criteria voor ZekeRE business of de Code van Informatiebeveiliging);
* of bij de rapportage moeten worden gevoegd (zoals in een SAS 70-rapportage).

In het kader van een assuranceopdracht zullen de criteria aan de volgende eigenschappen moeten voldoen, conform de (herziene) ISA100 ([IFAC03]):
* *relevantie*. Door relevante criteria te hanteren wordt bijgedragen aan het trekken van conclusies die beantwoorden aan het doel van de opdracht. Bovendien dragen zij bij aan de kwaliteit en/of inhoud van het object van onderzoek en daarmee aan de kwaliteit van de besluitvorming door de beoogde gebruikers.
* *betrouwbaarheid*. Door betrouwbare criteria te hanteren wordt bereikt dat beroepsbeoefenaren die over vergelijkbare deskundigheid beschikken, onder vergelijkbare omstandigheden zullen komen tot een redelijk consistente toetsing, evaluatie, en indien relevant presentatie van het object van onderzoek, respectievelijk tot redelijk consistente conclusies daaromtrent.
* *neutraliteit*. Criteria zijn niet neutraal indien door ze te hanteren de gebruikers van een assurancerapport worden misleid.
* *begrijpelijkheid*. Begrijpelijke criteria zijn duidelijk en allesomvattend en kunnen niet op significant verschillende wijzen worden geïnterpreteerd.
* *volledigheid*. Criteria zijn volledig indien alle criteria die in beginsel van invloed kunnen zijn op de conclusies, daadwerkelijk geïdentificeerd, ontwikkeld en gebruikt zijn.

De NOREA heeft in *Studierapport 3* ([NORE02b]) een eigen aanzet gegeven tot het ontwikkelen van dergelijke metanormen. Hierin is vermeld dat de metanormen betrekking hebben op:
* *objectiviteit:* de mate waarin normen(stelsels) vrij zijn van persoonlijke beïnvloeding;
* *eenduidigheid:* de mate van precisering en eenduidigheid van formulering;
* *relevantie:* de mate waarin normen(stelsels) bruikbaar zijn voor bepaalde auditopdrachten;
* *herleidbaarheid:* de mate waarin kan worden vastgesteld waaraan normen(stelsels) zijn ontleend;
* *zorgvuldigheid:* de mate waarin het normenstelsel beantwoordt, al dan niet juridisch verankerd, aan de maatschappelijke opvattingen over behoorlijk IT-gebruik.

In het kader van dit artikel voert het te ver om de overeenkomsten en verschillen van deze metanormen verder uit te werken.

Indien geen geschikte criteria beschikbaar zijn voor het onderkende onderzoeksobject dan kan mogelijk (conform de herziene ISA100 ([IFAC03])):
* een component van het onderzoeksobject waarvoor wel geschikte criteria beschikbaar zijn als onderzoeksobject worden gehanteerd. Zorgvuldigheid is in dergelijke situaties noodzakelijk om ervoor te zorgen dat het onderzoeksobject in het rapport niet wordt verward met het oorspronkelijke onderzoeksobject;
* wel een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden worden verleend.

Bij het 'afpellen' van het oorspronkelijke onderzoeksobject tot een onderzoeksobject waarvoor wel een toereikende set van criteria voorhanden is, moet ervoor worden gezorgd dat de opdracht (onderzoek van het specifieke onderzoeksobject) nog aansluit op de veronderstelde behoeften van de gebruikers.

De Code voor Informatiebeveiliging is in dit verband noemenswaardig. Deze code is breed geaccepteerd als de leidraad voor het opzetten en implementeren van informatiebeveiliging. Maar binnen het vakgebied van IT-auditing wordt de Code voor Informatiebeveiliging niet altijd als normenset beschouwd, maar soms slechts als 'best practice' waaruit de (concrete en op het onderzoeksobject toegesneden) normen kunnen worden afgeleid. De Code voor Informatiebeveiliging is ontwikkeld voor een brede toepasbaarheid en omvat een breed maar enigszins globaal raamwerk, en is daardoor vaak minder gerelateerd aan specifieke IT-objecten. Toch kunnen organisaties die voldoen aan de Code van Informatiebeveiliging hiervoor wel gecertificeerd worden (BS 7799). Hierbij is dan het managementsysteem het onderzoeksobject en niet de processen en/of de dienstverlening waarbinnen diverse beveiligingsmaatregelen zijn getroffen. Het abstractieniveau van het onderzoeksobject is daardoor vele malen hoger.

Reikwijdte opdracht

Bij TPM-opdrachten moeten wij ons afvragen of de opdrachtomschrijving en de TPM aansluiten op het ervarings- en kennisniveau en de behoeften van de beoogde gebruikers. De IT-auditor moet dan ook de beoogde gebruikers en hun doel onderkennen. Indien alleen triviale managementbeweringen moeten worden getoetst, die niet aansluiten op het doel van de beoogde gebruikers (naar de mening van de IT-auditor), dan mag dit soort opdrachten niet worden aanvaard.

Onder reikwijdte worden mede verstaan de opzet, het bestaan en/of de werking van het onderzoeksobject. Dit zijn begrippen die tot het auditorsjargon behoren en die binnen het auditorsberoep ook wel verschillend worden gedefinieerd. Een voorbeeld waar geen eenduidig onderscheid tussen opzet en bestaan wordt gemaakt, is te vinden in RAC 402 ([NIVR02]). Hierin is vermeld dat er in het algemeen twee verschijningsvormen bestaan van rapporten van accountants van serviceorganisaties, een Type A- en een Type B-rapport. Een Type A-rapport betreft een rapport inzake de toereikendheid van de *opzet*. Hierbij is echter tevens aangegeven dat in zo'n rapport ook een mededeling wordt gedaan dat de controlemaatregelen in de systemen operationeel zijn (= *bestaan*). Het eenduidig definiëren en gebruiken van dergelijke begrippen of ze eventueel vermijden is dan ook essentieel.

De opzet heeft betrekking op het ontwerp van de maatregelen en omvat derhalve de formele inrichting van het onderzoeksobject, zoals vastgelegd in organisatieschema's, procedurebeschrijvingen, systeemspecificaties en handboeken. Het bestaan betreft de daadwerkelijke uitvoering van de geïmplementeerde beheersingsmaatregelen op enig moment. De werking ten slotte is het bestaan van de maatregelen gedurende een bepaalde periode.

Het gebruik van deze termen kan bij het maatschappelijk verkeer leiden tot een verwachtingskloof, met name indien niet de werking of slechts enkel de opzet wordt getoetst. Een dergelijke opdracht waarbij alleen maar de opzet wordt getoetst, lijkt dan ook slechts verdedigbaar indien een dergelijke beperkte reikwijdte met de beoogde gebruiker(s) is afgestemd, die bovendien het beperkte karakter van een dergelijke opdracht moet(en) kunnen doorgronden. Dit kan dus alleen indien er sprake is van één bekende gebruiker of een beperkte kring van bekende gebruikers.

Managementbewering ('assertion-based'-opdracht)

Een managementbewering is een uitspraak van het management over het onderzoeksobject. Bij een 'assertion-based'-opdracht heeft de TPM betrekking op deze managementbewering en niet rechtstreeks op het onderzoeksobject, zoals bij een 'direct reporting'-opdracht het geval is. Voor het onderzoek zelf maakt dit onderscheid niet of nauwelijks verschil.

De IT-auditor moet de beoogde gebruikers en hun doel onderkennen.

In SSAE10 (AT Section 101 Attestation Engagements van [AICP01]) is bepaald dat bij iedere 'Attestation Engagement' een managementbewering opgesteld moet worden. WebTrust en SysTrust zijn vormen van 'Attestation Engagements' en bij dit soort opdrachten is een managementbewering dan ook verplicht. Hoewel bij dit soort opdrachten tijdens de opdrachtuitvoering een managementbewering dient te worden verkregen, kan nog wel een 'direct reporting'-opdracht worden uitgevoerd. De managementbewering is dan 'slechts' een onderdeel van het controlebewijs. Bij dit soort situaties is nog wel aangegeven dat de auditor wel om de publicatie van de managementbewering kan verzoeken.

Het voordeel van een 'assertion-based'-opdracht is dat de betrokkenheid en de verantwoordelijkheid van het management voor het onderzoeksobject expliciet worden gemaakt. Het is daarom wenselijk dat TPM-opdrachten, met name ten behoeve van (deels) onbekende gebruikers (maatschappelijk verkeer) als een 'assertion-based'-opdracht worden uitgevoerd. Een uitzondering kan worden gemaakt voor pakketcertificering.

<verantwoordelijke partij> managementbewering
Wij zijn verantwoordelijk voor het stelsel van maatregelen met betrekking tot <proces>, inclusief de in het systeem opgenomen maatregelen. Wij hebben maatregelen getroffen ter waarborging van de betrouwbaarheid en continuïteit van dit proces. De criteria die hieraan gesteld kunnen worden, zijn beschreven in een normenkader <referentie naar criteria>.

Wij verklaren hierbij dat de getroffen maatregelen in opzet voldoen aan de gestelde criteria. Tevens verklaren wij dat deze maatregelen op <datum> daadwerkelijk zijn geïmplementeerd.

<datum, plaats>, Management <verantwoordelijke partij>

Kader 3a. Managementbewering.

Bij pakketcertificering is het onderzoeksobject statisch en niet aan verandering onderhevig. De getroffen beheersingsmaatregelen in een softwarepakket zijn technisch van aard en minder beïnvloedbaar door het management. De noodzaak voor een 'assertion-based'-opdracht bij pakketcertificering is hierdoor minder aanwezig.

Kader 3b. TPM naar aanleiding van de managementbewering.

Third-partymededeling

Opdracht
In opdracht van <opdrachtgever> heeft <opdrachtnemer> een audit uitgevoerd naar de managementbewering van <verantwoordelijke partij>.

In deze bewering verklaart het management van <verantwoordelijke partij> dat de getroffen beheersingsmaatregelen ter waarborging van de betrouwbaarheid en continuïteit van <proces> in opzet voldoen aan de gestelde criteria <referentie naar criteria>. Ook verklaart het management dat deze beheersingsmaatregelen op <datum> daadwerkelijk zijn geïmplementeerd.
Onder betrouwbaarheid en continuïteit is in dit verband te verstaan de redelijke zekerheid dat transacties juist en tijdig worden verwerkt, dat het <proces> continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.

Onze audit was erop gericht met redelijke mate van zekerheid vast te stellen of de bijgevoegde bewering van het management van <verantwoordelijke partij> een getrouwe weergave is van de feitelijke situatie op <datum>.

Het management van <verantwoordelijke partij> is verantwoordelijk voor het instellen en onderhouden van een effectief stelsel van beheersingsmaatregelen en voor de managementbewering hierover. Het is onze verantwoordelijkheid hierover een oordeel te verstrekken op basis van het door ons uitgevoerde onderzoek.

Werkzaamheden
Onze audit is verricht in overeenstemming met algemeen aanvaarde standaarden voor assuranceopdrachten. Onze werkzaamheden hebben wij zodanig gepland en uitgevoerd, dat een redelijke mate van zekerheid wordt verkregen voor het afgeven van ons oordeel. Onze werkzaamheden omvatten onder meer interviews, documentatiebeoordeling en deelwaarnemingen op de uitvoering van maatregelen en andere auditprocedures uitgevoerd die wij noodzakelijk achtten.

Het onderzoek is uitgevoerd in de periode <maand(en)/jaar>. Wij zijn van mening dat onze werkzaamheden een deugdelijke grondslag vormen voor ons oordeel.

Oordeel
Op grond van ons onderzoek zijn wij van oordeel dat de bijgevoegde managementbewering een getrouwe weergave is van de feitelijke situatie op <datum>, in overeenstemming met de vastgestelde criteria.

<Eventuele nadere toelichting>

<ondertekening>

Een voorbeeld van een managementbewering en de TPM daarover omtrent de opzet en het bestaan van bepaalde maatregelen is in kader 3a respectievelijk 3b opgenomen.

Bevestigingsbrief

Het hanteren van een bevestigingsbrief (of Letter of Representation) is nog geen goed gebruik binnen het vakgebied van IT-auditing in Nederland.

Een bevestigingsbrief is (naar analogie van RAC 580 ([NIVR02])) een schriftelijke mededeling van de leiding van de verantwoordelijke partij over de feiten en omstandigheden die voor het oordeel van de IT-auditor van materieel belang zijn, terwijl in redelijkheid niet kan worden verwacht dat omtrent deze feiten en omstandigheden andere toereikende informatie beschikbaar is.

Een dergelijke brief kan van de leiding van de verantwoordelijke partij worden gevraagd na afloop van de onderzoekswerkzaamheden maar vooraf aan het afgeven van de TPM.

Op het eerste gezicht lijkt de toegevoegde waarde van zo'n bevestigingsbrief beperkt. Echter, in zo'n brief kan expliciet de verantwoordelijkheid voor het onderzoeksobject worden benadrukt. Natuurlijk dient een IT-auditor zodanig zijn onderzoek te plannen en uit te voeren dat hij voldoende zekerheid krijgt omtrent het onderzoeksobject, maar het is ineffectief zo niet onmogelijk om alle mogelijke relevante informatie tijdens het TPM-onderzoek te bestuderen. De verantwoordelijke partij is als geen ander op de hoogte van de mate waarin beheersingsmaatregelen zijn getroffen en effectief zijn gebleken. Daarom zal in de bevestigingsbrief ook aan de verantwoordelijke partij gevraagd worden of bij deze geen omstandigheden en informatie bekend zijn (denk bijvoorbeeld aan side-letters, of gebeurtenissen na de periode waarop de TPM betrekking heeft) die zouden kunnen leiden tot een andersluidend oordeel van de IT-auditor. Tevens kan in de bevestigingsbrief de doelgroep expliciet worden vermeld.

Een bevestigingsbrief is dan ook voor alle TPM-opdrachten een zinvolle en wellicht een noodzakelijke wijze om het onderzoek af te sluiten. In kader 4 is een voorbeeld van een bevestigingsbrief opgenomen.

De zinsnede omtrent de verantwoordelijkheid voor de inrichting van het stelsel van maatregelen ter waarborging van <kwaliteitsaspecten> van het <onderzoeksobject> is bij een 'assertion-based'-opdracht minder relevant omdat deze verantwoordelijkheid reeds in de managementbewering tot uitdrukking komt. De rest van

(Briefhoofd van verantwoordelijke partij)

Aan <opdrachtnemer>

(Adres)

Plaats, datum

Mijne heren,

Deze bevestiging wordt afgegeven in samenhang met uw onderzoek van de ... (kwaliteitscriteria en onderzoeksobject) van ... (naam verantwoordelijke partij) over de periode ..., dat gericht is op het afgeven van een Third Party Mededeling (TPM).
Wij erkennen onze verantwoordelijkheid voor de inrichting van het stelsel van maatregelen ter waarborging van <kwaliteitsaspecten> van het <onderzoeksobject>.

Wij bevestigen naar ons beste weten, per ... 200x, de datum van uw rapport, het volgende:
* Wij hebben u toegang verschaft tot alle relevante informatie die van invloed is geweest op de keuze van veronderstellingen en uitgangspunten die relevant zijn voor uw onderzoek.
* Wij onderschrijven de conclusie in uw rapport en/of TPM, en bij ons zijn geen omstandigheden en informatie bekend die zouden kunnen leiden tot een andersluidend oordeel.
* De TPM is bestemd voor <doelgroep> en zal zonder uw voorafgaande schriftelijke toestemming niet verder worden verspreid.

Hoogachtend,

(naam van de verantwoordelijke partij)

Kader 4. Voorbeeld van een bevestigingsbrief.

Third Party Mededeling voor:
<<verantwoordelijke partij>>
ten aanzien van:
Services verleend aan klanten voor wat betreft
<<dienstverlening>>

Opdracht
In opdracht van <opdrachtgever> heeft <opdrachtnemer> een audit uitgevoerd naar het stelsel van maatregelen ter waarborging van de betrouwbaarheid en continuïteit van [objectomschrijving: het proces en informatiesysteem (en/of interfaces)].
Onder betrouwbaarheid en continuïteit is in dit verband te verstaan de redelijke zekerheid dat transacties juist en tijdig worden verwerkt en dat het <object> continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.
Onze audit was erop gericht met redelijke mate van zekerheid vast te stellen dat het stelsel van maatregelen in opzet voldoet aan de normen zoals opgenomen in [Referentie naar Uitbestedingscontract / Referentie Sound Practices / Referentie naar specifiek normenkader dat opvraagbaar is bij opdrachtgever of ondergetekende]. Onze audit was er tevens op gericht vast te stellen of de maatregelen op het moment van ons onderzoek effectief waren geïmplementeerd.
Het stelsel van maatregelen ter waarborging van de betrouwbaarheid en continuïteit van [objectomschrijving: het proces en informatiesysteem (en interfaces)] is ingericht onder verantwoordelijkheid van <verantwoordelijke partij>. Het is onze verantwoordelijkheid hierover een oordeel te verstrekken.

Werkzaamheden
Onze audit is verricht in overeenstemming met algemeen aanvaarde standaarden voor assuranceopdrachten. Onze werkzaamheden hebben wij zodanig gepland en uitgevoerd, dat een redelijke mate van zekerheid wordt verkregen voor het afgeven van ons oordeel. Onze werkzaamheden omvatten onder meer interviews, documentatiebeoordeling en deelwaarnemingen op de uitvoering van maatregelen en andere auditprocedures die wij noodzakelijk achtten.
De audit is uitgevoerd in de periode [maand(en)/jaar]. Wij zijn van mening dat onze werkzaamheden een deugdelijke grondslag vormen voor ons oordeel.

Oordeel
Op grond van ons onderzoek zijn wij van oordeel dat het stelsel van maatregelen ter waarborging van de [kwaliteitsaspecten:xyz] van [objectomschrijving: proces en informatiesysteem (en interfaces)] in opzet voldoet aan de gestelde normen. Tevens zijn wij van oordeel dat de maatregelen op [datum] effectief waren geïmplementeerd.

<Eventuele nadere toelichting>

<ondertekening>

Kader 5. Voorbeeld TPM-rapport met goedkeurend oordeel in beknopte vorm.

Beoogde gebruikers	Mate van zekerheid	Reikwijdte	Management-bewering	Bevestigings-brief	Verschijnings-vorm
Eén bekende gebruiker of een beperkte kring van bekende gebruikers	Audit, review of opdracht tot het verrichten van overeengekomen specifieke werkzaamheden	Opzet is mogelijk, mits beoogde gebruiker beperkte strekking hiervan kan doorgronden	Optioneel	Zinvol	Uitgebreid of beknopt
(Deels) onbekende gebruikers	Audit	Minimaal opzet en bestaan	Verplicht	Zinvol	Beknopt of uitgebreid

Tabel 1. Kenmerken van een TPM-opdracht/rapportage per gebruikersgroep.

de inhoud van de bevestigingsbrief is ook voor een 'assertion-based'-opdracht van belang.

Rapportage

Bij TPM-opdrachten kunnen de volgende rapportagevormen worden onderkend:
- beknopt;
- uitgebreid.

Een rapportage in beknopte vorm bestaat in essentie uit een aanduiding van het onderzoeksobject, een oordeel en een verwijzing naar de vindplaats van de normen. Een rapportage in beknopte vorm is bijvoorbeeld een certificaat, zoals in kader 5 is opgenomen.

Een rapportage in beknopte vorm is uitsluitend mogelijk indien de gebruikers toegang hebben tot het normenstelsel. Bij een TPM-opdracht in de vorm van overeengekomen specifieke werkzaamheden (OSW) worden de uitkomsten in een rapport van (feitelijke) bevindingen vermeld, waarin geen oordeel of conclusie is opgenomen.

Een rapportage in uitgebreide vorm is conform een regulier IT-auditrapport, met dien verstande dat aan de opdrachtgever toestemming wordt verleend om het rapport aan de beoogde gebruiker(s) te verstrekken. Het rapport kan naast de normen ook de bevindingen (al dan niet voor iedere norm) bevatten alsmede een uitvoerige beschrijving van het onderzoeksobject en een beschrijving van de uitgevoerde werkzaamheden. Een voorbeeld van een uitgebreide TPM is een SAS 70-rapport. In de oordeelsparagraaf van een uitgebreid rapport moeten de elementen terugkomen die in het voorbeeld van een beknopt rapport (zie kader 5) zijn vermeld.

Een rapportage in uitgebreide vorm kan ook naast een TPM (of rapport in beknopte vorm) uitsluitend ten behoeve van de verantwoordelijke partij worden uitgebracht. Op deze wijze wordt inzicht gegeven in de detailbevindingen die de verantwoordelijke partij kan gebruiken om haar dienstverlening te verbeteren.

Een rapport in beknopte vorm is meer geschikt voor (deels) onbekende gebruikers (maatschappelijk verkeer). Dan wordt op korte en bondige wijze het oordeel van de IT-auditor weergegeven. Voor één bekende gebruiker of een beperkte kring van bekende gebruikers kan een rapportage in uitgebreide vorm geschikter zijn. Juist bij een dergelijke doelgroep gaat het vaak niet alleen om het oordeel maar ook om het geven van inzicht op welke wijze de verantwoordelijke partij de in de TPM-opdracht genoemde doelstellingen bereikt. Hierbij is sprake van meer interactie tussen de IT-auditor, de gebruiker en de verantwoordelijke partij.

Samenvatting

In dit artikel is een overzicht gegeven van de verschillende facetten van een TPM-opdracht. Een TPM-opdracht is hierin gedefinieerd als een assuranceopdracht of een opdracht tot het verrichten van overeengekomen specifieke werkzaamheden (OSW) waarbij de gebruiker van de TPM niet tot dezelfde organisatie behoort als de verantwoordelijke partij voor het onderzoeksobject, of daartoe op vergelijkbare afstand staat (in concernverband).

Bij een assuranceopdracht wordt tevens onderscheid gemaakt tussen een audit en een review, waarbij een redelijke respectievelijk beperkte mate van zekerheid wordt verkregen of het onderzoeksobject voldoet aan de gestelde criteria. Aangegeven is dat de termen audit en review tegenwoordig niet uitsluitend behoren tot het domein van de accountant in het kader van de jaarrekeningcontrole.

In het artikel zijn verder diverse aspecten nader toegelicht en zijn enkele voorbeelden gegeven. Bij een TPM-opdracht kunnen twee gebruikersgroepen worden onderscheiden, daar waar sprake is van één bekende gebruiker of beperkte kring van bekende gebruikers en een groep met (deels) onbekende gebruikers. De belangrijkste aspecten zijn in tabel 1 per gebruikersgroep kort weergegeven.

Literatuur

[AICP01]
American Institute of Certified Public Accountants (AICPA), *Statements on Standards for Attestation Engagements 10 (SSAE10)*, 2001.

[FEDE03]
Fédération des Experts Comptables Européens, FEE Issue Paper, *Principles Of Assurance: Fundamental Theoretical Issues With Respect to Assurance in Assurance Engagements*, april 2003.

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

[IFAC01]
International Federation of Accountants (IFAC), *Code Of Ethics For Professional Accountants*, november 2001.

[IFAC02]
International Auditing and Assurance Standards Board, Study 1, *The determination and Communication of Level of Assurance Other than High*, issued by the International Federation of Accountants, juni 2002.

[IFAC03]
International Federation of Accountants, Exposure Draft Assurance Engagement, *Proposed 'International Framework For Assurance Engagements', Proposed ISAE 2000 'Assurance Engagements On Subject Matters Other Than Historical Financial Information' and Proposed Withdrawal of ISA 120 'Framework of International Standards on Auditing', to Replace International Standard on Assurance Engagements 100, Assurance Engagements*, maart 2003.

[ISAC02]
Information Systems Audit and Control Association (ISACA), *IS Auditing Guideline, Reporting Document #070.010.010*, 2002.

[Keij02]
Mw. S. Keijl RA CISA, *SAS 70 en SysTrust, Internationale Standaarden voor third party assurance bij IT-serviceorganisaties*, de EDP-Auditor, nummer 3, 2002.

[NIVR01a]
Koninklijk Nederlands Instituut van Registeraccountants, *Handboek EDP-Auditing*, Wolters Kluwer 2001.

[NIVR01b]
Koninklijk Nederlands Instituut van Registeraccountants, Audit Alert 11: *Werkzaamheden accountant in het kader van de Regeling Organisatie en Beheersing (ROB) van De Nederlandsche Bank*, 2 augustus 2001.

[NIVR02]
Richtlijn voor Accountantscontrole (RAC), editie 2002.

[NORE02a]
Nederlandse Orde van EDP-Auditors (NOREA), *Jaarboek 2002*, Hoofdstuk 3 'Oordelen', 2002.

[NORE02b]
Nederlandse Orde van EDP-Auditors (NOREA), Studierapport 3, *Raamwerk voor ontwikkeling normenstelsels en standaarden*, december 2002.

[NORE03]
Nederlandse Orde van EDP-Auditors (NOREA), *Jaarboek 2003*, Hoofdstuk 3 "'IT-audit Ethics' en de 'Sarbanes-Oxley Act'", 2003.

[Velt95]
Drs. P. Veltman RE RA, *Third party review en -mededeling bij uitbesteding van IT-services*, Compact, september 1995.

Drs. R.J.M. van Langen RE RA
is als senior manager werkzaam bij KPMG Information Risk Management. Hij heeft een uitgebreide ervaring op het gebied van beoordelen van (IT-gerelateerde) systemen en processen. Thans houdt hij zich binnen KPMG met name bezig met de ontwikkeling van vaktechniek.

vanlangen.ronald@kpmg.nl