Ervaringen van een netwerkserviceprovider met third-partymededelingen

Drs. J.G.M. Janssen RE MIM

Een betrouwbaar datanetwerk is voor het management van veel organisaties van levensbelang. Veel bedrijfsprocessen bij middelgrote en grote organisaties zijn volledig afhankelijk van de permanente beschikbaarheid van een goed beveiligd netwerk. Zeker wanneer een bedrijf landelijk of internationaal opereert is het netwerk niet alleen van jezelf, maar wordt gebruikgemaakt van een netwerkserviceprovider. KPN opereert in Nederland als één van de grootste netwerkserviceproviders. Dit artikel gaat na op welke wijze het management van zowel de opdrachtgevende partij als de serviceproviderpartij een bijdrage kan leveren aan het vertrouwen in de kwaliteit van het netwerk. Specifiek wordt ingegaan op de rol van onafhankelijke kwaliteitstoetsing in de vorm van een TPM. Bij een third-partymededeling geeft een onafhankelijke (derde) auditinstantie een oordeel (TPM) over de kwaliteit van de beheerprocessen, de informatiebeveiliging en de daarmee gerelateerde besturing van de (netwerk)dienstverlening van KPN aan klantorganisaties.

Inleiding

Rondom het beheer van netwerken bestaan veel vragen. Door de steeds toenemende eisen van gebruikers en klanten aan de continue beschikbaarheid van applicaties en netwerken moeten op een aantal vragen ondubbelzinnige antwoorden worden gegeven.

- Welk deel van ons netwerk is in eigen beheer en welk deel van het netwerk is uitbesteed? En aan wie is dat uitbesteed?
- Is dat wel een betrouwbaar bedrijf, zeker in deze tijd van toenemende onzekerheid over de continuïteit van de dienstverlening?
- Reageert het bedrijf wel snel genoeg op de wensen van de klanten en doen ze dat tegen redelijke kosten?
- Welke eisen worden gesteld aan het beheer en de beveiliging van het eigen netwerk en wanneer is dat voor de laatste keer getest?
- Zijn ook eisen gesteld aan de beveiliging en het beheer van het netwerk van de serviceprovider? En informeert de netwerkserviceprovider ons wel goed over de kwaliteit van het beheer en de beveiliging?
- Op welke wijze kunnen we meer zekerheid verkrijgen of de serviceprovider dit wel goed en veilig doet?
- Hoe stellen wij onze interne klanten, de eindgebruikers, gerust? Is dan alleen een TPM voldoende, of moeten we daar meer voor doen?

De overheid en landelijk en internationaal opererende bedrijven hechten grote waarde aan een goed beheerd en beveiligd netwerk.

Vragen die de laatste jaren steeds vaker gesteld worden aan netwerkserviceproviders. Zeker de overheid en landelijk en internationaal opererende bedrijven hechten grote waarde aan een goed beheerd en beveiligd netwerk. Maar wat is dan *goed beheerd en beveiligd*?
Het klinkt zo vanzelfsprekend, maar dat is het natuurlijk niet.
Is goed wel goed genoeg? En wat verstaat de netwerkserviceprovider precies onder beheer en beveiliging? Is dat wel goed vastgelegd en welke informatie hebben we over de getroffen maatregelen? Trouwens, wat kost dat wel niet, een *goed beheerd* en *beveiligd* netwerk? Voor je het weet wordt de boel in gewapend beton gestort en kan het netwerk nauwelijks nog worden aangepast aan nieuwe wensen uit de business. En hoe is dat dan in het contract vastgelegd?

Waaraan moet men denken bij een goed beheerd en beveiligd netwerk?

Vanzelfsprekend is het belangrijkste kwaliteitscriterium van een netwerk het kunnen beschikken over *voldoende bandbreedte* (bijvoorbeeld 155 Mb/s) tegen een *redelijke prijs*. Deze moet *snel aangepast* kunnen worden aan zich wijzigende behoeften (upgrading en downsizing). Maar ook de *permanente beschikbaarheid* (vaak oplopend tot 99,95%) en het snel *oplossen van verstoringen*.
Wat de laatste tijd steeds belangrijker wordt, is de *beveiliging* tegen inbreuken van buiten af. Vaak worden de eisen aan het netwerk kort samengevat met de volgende termen:

Een kwalitatief goed netwerk is:
effectief, efficiënt, beschikbaar, flexibel, beveiligd.

Een hele mond vol en niet zomaar één, twee, drie te realiseren. Daar moet wel een plan voor worden opgesteld.

Deze zaken moeten allereerst binnen de opdrachtgevende organisatie goed geregeld worden. Keuzen worden gemaakt en voorschriften worden vastgelegd. Maar ook worden met de netwerkserviceprovider goede afspraken gemaakt. En daarbij geldt een oud koopmansgezegde:

'Alle waar is naar zijn geld'. Hoge kwaliteitseisen kosten nu eenmaal meer dan eenvoudige eisen.
Wat wordt er dan allemaal geregeld?
Meerdere partijen leveren hun inbreng, contractpartners kunnen elkaar in een goed overleg vinden op de gewenste kwaliteit tegen acceptabele kosten. Binnen de eigen organisatie moeten niet alleen de notoire contractonderhandelaars en juristen aan het roer staan. Ook de gebruikers en de eigen beheerders spelen een grote rol.
Bij volledige uitbesteding van het netwerkbeheer (zowel het technische beheer als het functionele beheer) worden meer kwaliteitseisen gesteld dan bij alleen de uitbesteding van het technische beheer.

Kwaliteitsbeheersing door de opdrachtgever (uitdagingen en valkuilen)

Om de kwaliteit van het netwerk bij uitbesteding te kunnen beheersen moeten bij de opdrachtgever in ieder geval de volgende twee centrale processen worden ingericht:
* bepalen van het gewenste kwaliteitsniveau;
* bewaken van de uitvoering.

Dat ziet er op het eerste gezicht eenvoudig uit, maar in de praktijk komt er nogal wat bij kijken. Laten we beide processen eens nader beschouwen.

Kwaliteitseisen moeten eenduidig en meetbaar zijn.

Bepalen van het gewenste kwaliteitsniveau

Voor het bepalen van het gewenste kwaliteitsniveau geeft de bedrijfsleiding van de opdrachtgever eerst aan hoe belangrijk de bedrijfsprocessen zijn voor de doelstellingen van de organisatie. Vaak is dat meer een zaak van gevoel en overtuiging dan van harde criteria. Om dan te komen tot een gemeenschappelijke visie is nog niet zo eenvoudig. Zeker niet als door marktontwikkelingen de doelstellingen en bedrijfsprocessen regelmatig veranderen. Van een stabiele situatie is eigenlijk al jaren geen sprake meer. Een globale indicatie van de processen en hun belang is dan al een hele prestatie.
Vervolgens wordt per bedrijfsproces nagegaan in welke mate het proces afhankelijk is van het netwerk. Dit houdt in dat een scherp zicht nodig is op de bedrijfsprocessen en dat de eigenaar van het proces (als het proces al een eigenaar heeft) precies weet wat de belangrijkste risico's zijn binnen het bedrijfsproces en welke beheersingsmaatregelen moeten worden getroffen. Ook hier geldt dat de benodigde informatie vaak niet direct beschikbaar is en dat vaak volstaan wordt met een globale indicatie, waarbij nog veel ruimte is voor interpretatie.
Het resultaat moet dan vertaald worden naar kwaliteitseisen aan het netwerk en de netwerkbeheerprocessen.
De volgende onderwerpen zijn hierbij van belang:

Kwaliteitseisen
Deze worden veelal benoemd in (de bijlagen bij) het contract voor de intern dan wel extern uit te besteden taken. Van belang hierbij is dat de eisen eenduidig en meetbaar zijn.

Service level agreement
Vaak zien we een service level agreement (SLA), waarin de kwaliteitseisen gespecificeerd worden, inclusief de rapportage items (key performance indicators). In de SLA is meestal een lijst met definities opgenomen. De eisen kunnen vervolgens nog in operationele afspraken en procesbeschrijvingen worden uitgewerkt.

Overlegvormen
De doelen van de verschillende overlegvormen en de wijze van escaleren bij spoed- en noodsituaties en bij meningsverschillen worden aangegeven.

Ontkoppelpunten/verantwoordelijkheden
Een essentieel, maar vaak onderbelicht onderwerp is het bepalen van de ontkoppelpunten tussen opdrachtgever en serviceprovider. Waar begint en eindigt de verantwoordelijkheid van de opdrachtgever, zowel in de opdrachtverlening als bij de uitvoering van de processen, en hoe zit dat voor de serviceprovider? Hier ontstaan vaak misverstanden die samengevat kunnen worden onder de volgende stelling: 'Het wat en het hoe van de dienstverlening worden door elkaar gehaald'. Eisen over te leveren diensten (het wat) worden vaak uitgelegd in eisen aan in te zetten personeel en te gebruiken technieken (het hoe). Daardoor ontstaat een vorm van 'dubbele besturing' die in het normale leven meestal tot ongelukken leidt. Sterk vereenvoudigd zijn er twee soorten contracten: Fixed price en Time&Material. Bij Fixed price-contracten worden afspraken gemaakt over budget en kwaliteit van de dienstverlening en wordt ook 'afgerekend' op de kwaliteit van de dienstverlening. Eisen aan de in te zetten mensen en materialen zijn minder expliciet. Bij een Time&Material-contract worden afspraken gemaakt over het budget voor in te zetten mensen en hulpmiddelen en wordt daar ook op 'afgerekend'. Hierbij worden minder harde afspraken over de gewenste kwaliteit gemaakt, vaak omdat partijen dat nog moeilijk kunnen aangeven. Zoals aangegeven zien we in de praktijk vaak de twee vormen door elkaar lopen, met als resultaat misverstanden en competentieproblemen.

Toezicht en controle
Bij het bepalen van het gewenste kwaliteitsniveau wordt vaak aangegeven of er sprake is van een vorm van verbijzonderd toezicht of controle, zoals periodieke inspectie of TPM's. Voor sommige vormen van netwerkdienstverlening bestaan wettelijke verplichtingen en is het verbijzonderd toezicht wettelijk geregeld. Maar voor het overgrote deel moeten tussen partijen specifieke afspraken worden gemaakt.

Bewaken van de uitvoering

Het bewaken van de kwaliteit van de uitvoering is een verantwoordelijkheid van de opdrachtgever. Terecht mag de opdrachtgever ervan uitgaan dat de serviceprovider zelf metingen verricht en periodiek informatie verschaft over de kwaliteit van de dienstverlening, zeker als daar in het contract goede afspraken over gemaakt zijn. Wederom is de praktijk weerbarstiger dan de theorie.

Hieronder wordt een aantal kritische aspecten van de bewaking beschreven.

In algemene zin zijn drie soorten bewaking (in de relatie opdrachtgever - provider) te onderscheiden:
1. periodieke rapportages;
2. periodiek overleg;
3. onafhankelijke oordeelsvorming.

1. Periodieke rapportages
De SLA beschrijft meestal uitvoerig de items waarover rapportages worden opgeleverd. Daarbij is vaak niet goed gedefinieerd aan welke betrouwbaarheidseisen (juistheid, tijdigheid en volledigheid) de rapportages moeten voldoen en welke toleranties acceptabel zijn. Vaak is niet aangegeven op welke wijze de rapportages worden afgehandeld en tot welke besluitvorming dit leidt (bijvoorbeeld een bonus-malussysteem). Hierdoor lopen de interesse en de discipline voor het opstellen en bespreken van periodieke rapportages vaak terug. Om te voorkomen dat de rapportages als een verplicht nummer afgedraaid worden, moeten duidelijke afspraken worden gemaakt over de afhandeling door het management van zowel de opdrachtgevende als de serviceproviderpartij.

2. Periodiek overleg
Wij leven in een overlegcultuur. Daarom zijn vaak vele vormen van overleg gedefinieerd op zowel strategisch, tactisch als operationeel niveau. Deze overleggen zijn veelal noodzakelijk om allerlei incidenten en voorvallen op een collegiale wijze af te handelen. Zonder afbreuk te willen doen aan de vele goed afgebakende en goed voorbereide overlegvormen doen zich ook situaties voor waarin de effectiviteit (lossen we de aangedragen problemen goed en snel op) door betrokkenen als gering wordt ervaren. Dit probleem treffen wij vaker aan bij de tactische en strategische overleggen dan bij de operationele overleggen. Veelal is er sprake van overlap in onderwerpen en onduidelijke verantwoordelijkheden en bevoegdheden. Gevolg is het regelmatig terugkomen van dezelfde kwaliteitsthema's op agenda's van verschillende overleggen. In de praktijk blijkt het beter te zijn het aantal overleggen terug te brengen tot één operationeel en één tactisch overleg en deze twee met een vaste frequentie te laten plaatsvinden.

3. Onafhankelijke kwaliteitstoetsing
Met name bij langlopende en omvangrijke contracten is het gebruikelijk dat afspraken worden gemaakt over het periodiek laten beoordelen van de kwaliteit van de dienstverlening door een onafhankelijke deskundige. Deze afspraken zijn enthousiast vastgelegd bij de contractonderhandelingen, maar in loop van de contractuitvoering is de naleving van de kwaliteitstoetsing nogal eens een gecompliceerd proces. Vaak heeft dit onderwerp ook geen verdere uitwerking gekregen in de verdere detaillering van de afspraken.

Kwaliteitsbeheersing door de serviceprovider

Bij de serviceprovider spelen bij de kwaliteitsbeheersing de volgende twee vragen een centrale rol:
* Spelen we voldoende in op de kwaliteitswensen van de klant?
* Hoe kunnen we dat inspelen op kwaliteit bestuurbaar en aantoonbaar maken?

Inspelen op de dagelijkse wensen van de klant

Essentieel hierbij is dat voldoende maatregelen in de processen en systemen worden getroffen om te voldoen aan de overeengekomen service levels. Belangrijke onderwerpen daarbij zijn:
* één resultaatverantwoordelijk aanspreekpunt;
* goed gedefinieerde koppelvlakken tussen de opdrachtgeverorganisatie en de serviceprovider;
* een goed bereikbare order- en helpdesk;
* een geoutilleerde back-office voor complexere klantvragen;
* eenvoudig hanteerbare en betrouwbare tools voor het verwerken van orders, informatievragen en incidenten;
* voldoende en goed opgeleid personeel om de klantvragen snel af te handelen;
* goed in de problematiek van de klantorganisatie ingewerkte adviseurs;
* indien nodig het snel kunnen inrichten van een deskundig projectteam om samen met de klantorganisatie veranderingen of uitbreidingen in het netwerk voor te bereiden en door te voeren;
* simpel leesbare en heldere rapportages;
* een overzichtelijke factuur, aangepast aan de informatiewensen van de klant;
* tijdige signalering van overbelasting van netwerkelementen;
* zorg dragen voor beveiliging van het netwerk;
* managen van interne dienstverleners en subcontractors.

De naleving van de kwaliteitstoetsing is nogal eens een gecompliceerd proces.

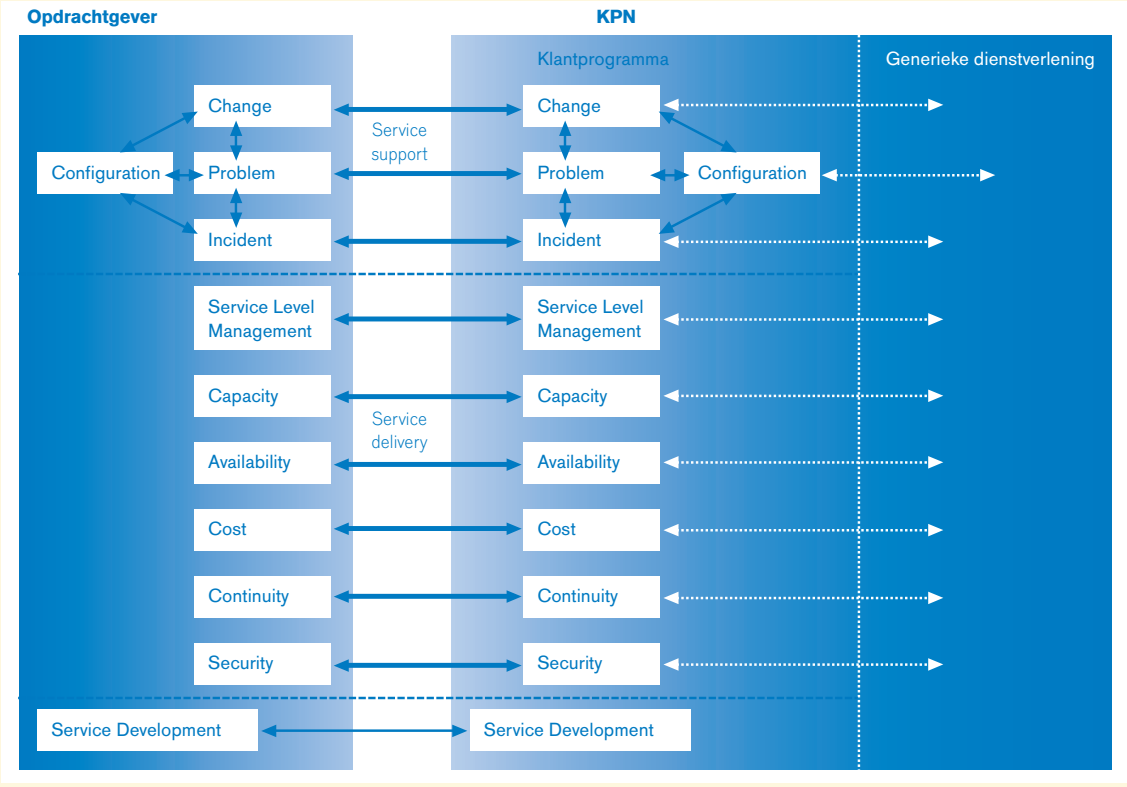
De meeste van deze wensen kunnen worden ingevuld met een adequate invoering van support- en deliveryprocessen van ITIL.

In figuur 1 op de volgende pagina worden deze principes weergegeven.

Het bestuurbaar en aantoonbaar maken van de kwaliteit

In de dagelijkse praktijk hoort men vaak dat een goede implementatie van ITIL borg staat voor een kwalitatief goede dienstverlening. ITIL dwingt immers een sterke onderlinge afstemming van de processen af, waardoor de beheersing als het ware vanzelf (inherent) afgedwongen wordt. Maar voor het bestuurbaar en aantoonbaar maken van de kwaliteit is meer nodig ...

Onmiskenbaar is het gedisciplineerd uitvoeren van de support- en deliveryprocessen de basis voor een kwalitatief goede dienstverlening. Maar hoe stel je nu vast wat goed is? Dit vereist duidelijk geformuleerde doelstellin-



Figuur 1. Koppelvlakken ITIL-processen.

gen en performance-eisen, al dan niet in de vorm van key performance indicators en een permanente monitoring door het management van de performance. Dit kan heel goed met een business balanced scorecard. De directe betrokkenheid van het management bij de dagelijkse werkzaamheden is vanzelfsprekend van groot belang. Ook het beschrijven van de processen en het opstellen van heldere werkinstructies dragen bij aan de bestuurbaarheid. En natuurlijk is het goed om in de verwerkingsprocessen een aantal controles in te bouwen, zodat we zeker weten dat we alle aanvragen op een juiste manier hebben verwerkt en er niet een vergeten hebben. En wanneer gebruik wordt gemaakt van de diensten van interne dienstverleners of subcontractors, is beheersing nodig. Zeker bij grote contracten zijn meerdere partijen betrokken. Dan is het van belang om systematisch de kwaliteit van de dienstverlening van deze partijen vast te stellen. Daarbij neemt de serviceprovider de rol aan van opdrachtgever.

Vaak beschouwen operationele managers deze zaken als 'overhead' en gedoe. Ze gaan nogal eens ten koste van de noodzakelijke capaciteit om te voldoen aan de dagelijkse klantvraag.
Maar ook bestaat er veelal onduidelijkheid over geleverde kwaliteit. Doen we het nu wel goed, of bieden we te weinig? Is de kritiek van de klant wel terecht?
Helder opgestelde maand- en jaarrapportages met een dito verschillenanalyse (wat hadden we beloofd en wat hebben we gerealiseerd?) creëren dan een hoop duidelijkheid. En verbeteracties dragen dan weer bij aan een hogere performance.

En als (externe) auditors langskomen om een onderzoek uit te voeren, dan kunnen ze voor hun oordeelsvorming goed gebruikmaken van deze controles, rapportages en analyses.

Vertrouwen blijft mensenwerk

Bij de start van een nieuw contract zijn de verwachtingen omtrent de samenwerking tussen de betrokken partijen vaak hooggespannen. Uit bovenstaande beschrijving blijkt dat de uitvoering van contractafspraken weerbarstig is en er snel tegenstellingen kunnen ontstaan. Op papier kunnen de afspraken nog zo helder zijn, in de dagelijkse praktijk doen zich velerlei situaties voor waardoor 'even afgeweken moet worden' van het afgesproken pad. Dan komt het vooral aan op de verhouding tussen de contractpartners of er 'een werkbare oplossing' wordt gevonden. Dit is zonder meer een leerproces voor partijen. Organisaties en processen moeten worden ingericht, informatiesystemen moeten worden aangepast en personeel moet worden opgeleid. Bij complexe diensten is dit een continu proces. Terecht kan worden gesproken van een lerende organisatie. Als de problemen zich echter opstapelen en de spanning toeneemt, komt het vooral aan op goede persoonlijke verstandhouding en begrip voor elkaars situatie. In zo'n sfeer van collegiaal overleg kunnen veel praktische problemen worden opgelost en groeit een sfeer van onderling vertrouwen. Van een lastig probleem kunnen dan de scherpe kantjes worden afgeslepen. Wanneer echter bij het eerste het beste voorval gedreigd wordt met claims, boetes en rechtszaken, is er eerder sprake van 'georgani-

seerd wantrouwen' en neemt de kans op een effectieve samenwerking af.

Aanvullende beheersingsmaatregelen, zoals extra detailrapportages of een gerichte kwaliteitsinspectie, worden vaak ingezet in situaties waarin de tegenstellingen hoog oplopen. Deze maatregelen kunnen natuurlijk nooit een vervanging zijn van een positieve probleemoplossende houding van contractpartners. Wel kunnen ze een bijdrage leveren aan het objectiveren van de ervaren probleemsituaties en een aanzet vormen voor een betere verstandhouding.

Beter is het de onafhankelijke kwaliteitstoetsing als een regulier onderdeel van de beheersing in te richten. Daarmee kunnen verrassingen worden voorkomen en levert kwaliteitstoetsing een systematische bijdrage aan de verbetering van de kwaliteit en vanzelfsprekend ook aan het onderling vertrouwen. In de volgende paragraaf wordt uit de doeken gedaan wat onafhankelijke kwaliteitstoetsing inhoudt en hoe die in de praktijk wordt vormgegeven.

De praktijk van reguliere onafhankelijke kwaliteitstoetsing

Drie vormen

In steeds meer contracten is een artikel of paragraaf opgenomen waarin afspraken tussen partijen worden gemaakt over onafhankelijke kwaliteitstoetsing. Daarbij doen zich veelal drie vormen voor:
1. het specifieke oordeel;
2. de third-partymededeling (TPM);
3. de TPM-plus.

1. Het specifieke oordeel
De *opdrachtgever* geeft, met instemming van de serviceprovider, opdracht aan een onafhankelijke auditinstantie, veelal één van de grote auditkantoren, om de kwaliteit van de specifiek voor de opdrachtgever ingerichte dienstverleningsprocessen bij de serviceprovider te beoordelen. Het oordeel wordt gegeven aan beide partijen.

2. Third-partymededeling (TPM)
Niet de opdrachtgever maar de *serviceprovider* geeft opdracht aan een onafhankelijke auditinstantie, wederom veelal één van de grote auditkantoren, om de kwaliteit van de generieke dienstverleningsprocessen bij de serviceprovider te beoordelen. Het oordeel wordt verstrekt aan het management van de serviceprovider die dit vervolgens, vergezeld van een toelichting, aanbiedt aan het management van de verschillende opdrachtgevers die diensten afnemen van de serviceprovider. Afhankelijk van de wensen van de opdrachtgever of de groep van opdrachtgevers kan aanvullend op het TPM-onderzoek de kwaliteit van specifieke objecten of processen worden getoetst.
Binnen KPN wint de praktijk van een TPM die toegesneden is op KPN Netwerkdiensten steeds meer terrein. De TPM voor KPN Netwerkdiensten is een normenkader voor de beoordeling van de kwaliteit van de netwerkdienstverlening van KPN aan met name grote klanten (corporate accounts). Naast de term TPM wordt binnen KPN ook de term Third Party Assurance (TPA) gebruikt.
In overleg met het management van de grote klanten en een aantal grote auditkantoren is een kader ontwikkeld waarmee in relatief korte tijd en dus tegen redelijke kosten de kwaliteit van de dienstverlening kan worden getoetst. Het TPM KPN-kader sluit aan bij internationale standaarden als ISO 17799 (Code voor Informatiebeveiliging), CobIT (Control Objectives for IT and related processes) en ITIL (Information Technology Infrastructure Library), maar kent ook specifieke kenmerken van het management van communicatietechnologie.
Het TPM KPN-kader kent de volgende hoofdgroepen voor beoordeling:
1. algemeen beheerbeleid en managementrapportages;
2. operationele beheerprocessen;
3. tactische beheerprocessen;
4. beheersing van de kwaliteit van de interne dienstverleners of subcontractors.

Geadviseerd wordt de onafhankelijke kwaliteitstoetsing als een regulier onderdeel van de beheersing in te richten.

3. De TPM-plus
Op verzoek van de *opdrachtgever* kan de onafhankelijke auditinstantie aanvullend op de TPM, zoals in punt 2 genoemd, voor nader te bepalen bedrijfskritische processen of diensten van de opdrachtgever, een beoordeling uitvoeren. Ook dit oordeel wordt verstrekt aan het management van de serviceprovider, die dit oordeel samen met de TPM en wederom met een eigen toelichting aanbiedt aan het management van de opdrachtgever.

Natuurlijk zijn er ook veel tussenvormen te onderkennen. Jammer genoeg komen er ook 'exoten' voor, waarbij de rolverdeling tussen opdrachtgever, serviceprovider en onafhankelijke auditinstantie onduidelijk is, dan wel rechten en plichten eenzijdig bij één van de partijen komen te liggen.

Nadere uitwerking

Aan iedere vorm van onafhankelijke oordeelsvorming kleven voor- en nadelen. En aan iedere vorm van TPM hangt ook een prijskaartje!

Het *specifieke oordeel* wordt gehanteerd wanneer er sprake is van een sterke afhankelijkheidsrelatie tussen opdrachtgever en serviceprovider en er zeer specifieke kwaliteitsafspraken zijn. Het nadeel van het specifieke oordeel is dat bij iedere wijziging van de dienstverlening en de kwaliteitsafspraken het onderzoek opnieuw moet worden uitgevoerd. Dit vraagt veel managementaandacht. De kosten van een specifiek oordeel zijn derhalve hoog. Veel vormen van netwerkdienstverlening hebben echter een meer generiek karakter en worden aangeboden aan meerdere partijen. In die gevallen is een speci-

Drs. J.G.M. Janssen RE MIM
is Lead IT Auditor bij KPN Audit en betrokken bij TPM-trajecten binnen KPN. Daarvoor was hij tien jaar werkzaam als controller en informatiemanager bij de Belastingdienst.

Dit artikel is geschreven op persoonlijke titel.
De auteur dankt George Hulst RE CISA (Lead IT Auditor KPN Audit), Theo Engelsma RE (Senior IT Auditor KPN Audit) en Herman van Gils RE RA (Senior manager KPMG IRM) voor hun bijdrage.

fiek oordeel niet noodzakelijk en kan volstaan worden met een TPM, al dan niet aangevuld met een oordeel over een beperkt aantal specifieke thema's.

De laatste jaren wint *TPM*, al dan niet vergezeld van de 'plus', steeds meer terrein. De mededeling die voortvloeit uit een TPM-onderzoek wordt door de serviceprovider verstrekt aan alle opdrachtgevers die belang hechten aan een dergelijke mededeling. Wanneer de TPM verstrekt wordt aan een groep van opdrachtgevers, vindt afstemming met (een vertegenwoordiging van) deze groep plaats. Als de TPM echter voor een breed publiek bedoeld is, wordt meer aangesloten bij algemene standaarden, zoals de Code voor Informatiebeveiliging. Bij de rijksoverheid bestaat al meer dan tien jaar ervaring met TPM'en ([Have89]).
Bij TPM'en wordt een actieve opstelling van de serviceprovider verwacht. Deze moet immers investeren in de borging van de dienstverleningsprocessen en deze processen door een onafhankelijke partij laten beoordelen. Zo'n onderzoek moet wel ieder jaar herhaald worden (voor de levensduur van de dienst). De onafhankelijke partij moet vanzelfsprekend erkend zijn door de verschillende opdrachtgevers. Daarom wordt veelal gekozen voor één van de grote auditkantoren. Vaak steunt de onafhankelijke auditpartij op de bij de serviceprovider uitgevoerde interne controles en interne audits. Dan worden er werkafspraken gemaakt tussen de externe auditpartij en de interne auditafdeling. Dit kan variëren van joint audits, externe review van uitgevoerde interne audits tot het zelfstandig uitvoeren van (steekproef)onderzoeken door de externe auditor. Afhankelijk van de te onderzoeken processen en objecten en afhankelijk van de beschikbare kennis en auditcapaciteit worden hier werkafspraken over gemaakt. De uitgevoerde onderzoeken moeten in alle gevallen voldoen aan de algemeen aanvaarde kwaliteitseisen voor 'assurance'-opdrachten ([NIVR02]).

Vertrouwen op je netwerk is goed, controleren is beter (maar zonder vertrouwen geen zinvolle controle).

Voor TPM-trajecten zijn daarbij drie zaken van belang:
1. De controle- en auditwerkzaamheden moeten voldoen aan algemene eisen van professionaliteit, onafhankelijkheid, zorgvuldigheid en aantoonbaarheid.
2. De gehanteerde kwaliteitsnormen moeten voor betrokken partijen bekend en door hen geaccepteerd zijn. Voor de te hanteren normen kan aangesloten worden op bestaande algemene internationale standaarden, zoals de Code voor Informatiebeveiliging en CobIT.
3. Er moet een duidelijke afbakening van de betrokken onderdelen van de dienstverlening zijn: welke objecten vallen binnen de scope en wat blijft daar nadrukkelijk buiten?

In de praktijk is er nog wel een aantal hobbels te nemen. Ook hier is het van belang dat bij partijen een basis van wederzijds vertrouwen bestaat en er een open communicatie is over de werkwijze en de te hanteren normen. Het is inmiddels een goed gebruik om één of twee keer per jaar in een gezamenlijk overleg van opdrachtgever, serviceprovider en onafhankelijke auditinstantie de aanpak en voortgang van de TPM-onderzoeken door te nemen. Vaak legt daarbij zowel de opdrachtgevende als de serviceproviderpartij een leertraject af. Daarbij doorlopen de organisaties volwassenheidsniveaus, beginnend bij (h)erkenning van het belang van beheersing via het op ad-hocbasis organiseren en het min of meer inregelen van processen tot continue meting en verbetering van de processen. Het is van belang dat beide partijen erkennen dat er sprake is van een leertraject. Het is immers niet mogelijk en vanuit het oogpunt van een goede borging van de dienstverleningsprocessen ook niet wenselijk dat geforceerd beheersingsmaatregelen worden opgelegd aan een organisatie. Veelal is dit soort maatregelen niet goed ingebed in de primaire bedrijfsprocessen en uiterst kostbaar. Het gevolg is dat deze 'verbijzonderde beheersingsmaatregelen' vaak niet lang standhouden en na verloop van tijd 'verwateren', waarna het hele liedje weer van voren af aan kan worden gezongen.

Conclusie

Vertrouwen op je netwerk is goed, controleren is beter (maar zonder vertrouwen geen zinvolle controle)

Als men niet kan vertrouwen op zijn netwerk, kunnen de dagelijkse werkzaamheden niet goed worden uitgevoerd, dat is inmiddels wel duidelijk. Steeds meer maatschappelijk kritische processen zijn afhankelijk van de betrouwbare werking van het bedrijfs- of het publieke netwerk. En dan gaat het niet alleen om de betrouwbaarheid van de technische werking van het netwerk, maar ook om de managementprocessen eromheen. Daarbij hangt veel af van de vertrouwensbasis tussen de opdrachtgevende organisatie en de netwerkserviceprovider. Vertrouwen houdt dan in openheid en helderheid over rechten en plichten en heldere afspraken over de wederzijdse naleving van de afspraken. Binnen zo'n vertrouwensrelatie hoort een afgewogen stelsel aan controles. Steeds meer neemt de netwerkserviceprovider zelf het initiatief tot het controleren en auditen van de dienstverleningsprocessen en het verstrekken van een onafhankelijk oordeel over de kwaliteit van de processen door middel van een TPM. Voor de betrokken partijen, zowel aan opdrachtgevers- als aan serviceproviderskant, is het vaak nog een leerproces om de beheersing goed in te richten. Beheersingsprocessen kunnen immers altijd naar een hogere volwassenheid doorgroeien.

Literatuur

[Have89]
M.E.G. ten Have RA RE, *Third Party Mededeling*, Financieel OverheidsManagement, 1989/12.

[NIVR02]
NIVRA, *Richtlijn voor de Accountantscontrole 100 'Assurance opdrachten'*, 2002.