Benchmarking van de general IT controls in de praktijk

Drs. J.C. de Boer RE en mw. ir. E.R. van Sommeren RE

Bij het uitvoeren van een systeemgerichte controle zal naast de beoordeling van de business-controls ook een beoordeling van de general IT controls plaatsvinden. Voor het vergroten van de toegevoegde waarde van de beoordeling kan gebruik worden gemaakt van IT Benchmarking. De praktijk wijst uit dat naast inzicht in betrouwbaarheid en continuïteit daadwerkelijk toegevoegde waarde wordt bereikt.

Inleiding

Enige jaren geleden is in Compact ingegaan op de mogelijkheid om benchmarking te gebruiken bij het beoordelen van de general IT controls ([Donk96]). Werd destijds vastgesteld dat benchmarking steeds meer in de belangstelling staat in Nederland, in de afgelopen jaren is die belangstelling alleen maar toegenomen. De invloed en betekenis van IT op organisaties stijgt en het management dient steeds sneller keuzen te maken op het gebied van IT. De vragen bij het management of de juiste keuzen worden gemaakt en hoe de general IT controls zich verhouden tot die van andere organisaties blijven echter aanwezig.

Dit heeft dan ook geleid tot het uitvoeren van benchmarkingonderzoeken op grotere schaal. De theorievorming is de afgelopen jaren omgezet in praktijkervaring en minstens even belangrijk is dat representatieve gegevensverzamelingen zijn opgebouwd die de basis voor het benchmarkproces vormen. Zo beschikt KPMG voor het benchmarken van de general IT controls inmiddels over een internationale database met gegevens van ongeveer 1800 organisaties. Deze gegevens zijn afkomstig uit verschillende landen, waardoor zowel nationale als internationale vergelijking mogelijk is.

Niet alleen organisaties hebben voordeel van de beschikbaarheid van deze bron van benchmarkinggegevens, ook in het kader van de jaarrekeningcontrole wordt volop gebruikgemaakt van de methodiek IT Benchmarking. Een belangrijke reden hiervoor is dat het gebruik van de methodiek IT Benchmarking de interpretatie van de resultaten 'makkelijker' maakt. Stukken tekst hebben plaatsgemaakt voor grafieken waardoor ook directies op een relatief eenvoudige wijze de risico's van IT voor een organisatie kunnen vaststellen. Daarnaast wordt de toegevoegde waarde van een onderzoek naar de general IT controls meer begrepen omdat naast de bevindingen van de IT-auditor ook de bevindingen van andere organisaties worden geplaatst.

In dit artikel wordt ingegaan op hoe benchmarking van de general IT controls wordt toegepast binnen de accountantscontrole. Tevens komen aan de orde de invloed die de uitkomsten kunnen hebben op de gehanteerde controleaanpak en de beleving van het management van de organisatie waar het onderzoek heeft plaatsgevonden. Dit wordt nader uiteengezet aan de hand van vier praktijkcases. Voorafgaand wordt kort behandeld wat benchmarking inhoudt en op welke wijze de general IT controls worden gebenchmarkt.

Wat is benchmarking?

Benchmarking kan worden gedefinieerd als het vergelijken van organisaties of organisatieonderdelen ([Pryo89]). Het is een continu, systematisch proces waarbij de resultaten van de vergelijking worden geëvalueerd. Benchmarking wordt veelal gebruikt als instrument om de performance van een organisatie te verhogen.

De resultaten van de vergelijking kunnen worden gebruikt als spiegelinformatie. De benchmarkinformatie is geen absolute norm maar dient te worden gebruikt voor het bewust maken van bedrijven en instellingen van het bestaan van verschillen tussen organisaties onderling, waarbij er in eerste instantie niet kan worden gesproken over 'goed' of 'fout'. Het advies is om te spreken van 'hoger' of 'lager' ten opzichte van de vergelijkingsmaatstaf. Nadere analyse moet uitwijzen of de door het benchmarkingproces daadwerkelijk geconstateerde verschillen acties tot gevolg moeten hebben.

Toepassing benchmarking bij IT-audits

Benchmarking kan op een aantal wijzen worden gebruikt bij IT-audits:

* benchmarking als zelfstandig onderzoek. Het benchmarkingproces wordt in samenwerking met een bedrijf of instelling uitgevoerd;
* benchmarking als extra hulpmiddel bij de financial, operational of IT-audits.

Indien een organisatie wil weten hoe haar positie is ten opzichte van andere soortgelijke organisaties kan, ten aanzien van de kwaliteitsaspecten van IT, een benchmarkingonderzoek worden uitgevoerd. Onder soortgelijk kan worden verstaan in dezelfde branche opererend of gebruikmakend van eenzelfde dan wel vergelijkbaar hardware/softwareplatform. Het is voor een organisatie vaak moeilijk om het benchmarkingproces zelfstandig uit te voeren omdat informatie over andere organisaties niet makkelijk verkrijgbaar is. Gezien de onafhankelijke positie van IT-auditors ten opzichte van organisaties en hun concurrenten biedt dit hen een uitstekende positie voor het uitvoeren van een dergelijk proces.

Naast een zelfstandig onderzoek kunnen de benchmarks ook als extra hulpmiddel worden gebruikt bij IT-audits. Een belangrijk voordeel hiervan is de overtuigingskracht die benchmarks met zich meebrengen. Elke IT-auditor weet dat het niet in alle gevallen eenvoudig is het management van organisaties te overtuigen dat de general IT controls aan bepaalde normen dienen te voldoen. Door organisaties naast een norm extra informatie te verschaffen over andere (soortgelijke) ondernemingen door middel van benchmarks blijkt dit overtuigen een stuk eenvoudiger te worden. Door een externe spiegel voor te houden wordt de discussie die doorgaans plaatsvindt over normen vaak ingewisseld voor vragen als: Wat moet er worden gedaan om de situatie te verbeteren? Doch evenzeer de vraag: Hebben wij niet te veel gedaan en benadelen we daardoor onze concurrentiepositie?

Benchmarks kunnen hierbij doelen dienen als:
* *referentiemateriaal*. Door het gebruik van benchmarks kunnen uitgangspunten voor onderzoek worden opgesteld door de sterkte(n) en zwakte(n) ten opzichte van andere organisaties in kaart te brengen. Dit overzicht kan behulpzaam zijn bij het opstellen van de aandachtspunten ten behoeve van de management letter en mogelijk kunnen prioriteiten van de te ondernemen activiteiten worden aangegeven;
* *ondersteuning van aanbevelingen*. Als op basis van onderzoek aanbevelingen zijn opgesteld, kunnen de benchmarks worden gebruikt als ondersteunende gegevens;
* *'eye-opener'*. Benchmarks kunnen zeer goed worden gebruikt voor het leveren van aanknopingspunten voor verbetering. Het feit dat andere organisaties een hogere score bereiken zal een organisatie er meer van overtuigen dat wegen tot verbetering bestaan;
* *monitoring*. Door periodiek een benchmark uit te voeren kunnen verbeteringen door de jaren heen worden gemeten. Tevens kan het als middel worden gebruikt om te zien of de betreffende organisatie geen achterstand oploopt ten opzichte van andere organisaties.

Benchmarks leveren organisaties een aanzienlijke hoeveelheid marktinformatie op waardoor het gebruik ervan in zijn algemeenheid als een toegevoegde waarde aan de audit kan worden gezien.

Benchmarking van general IT controls

In het vervolg van dit artikel wordt allereerst kort ingegaan op de general IT controls. Vervolgens wordt het algemene benchmarkingproces rondom de general IT controls en de hulpmiddelen die daarvoor binnen KPMG worden ingezet, nader besproken. Daarna worden aan de hand van een viertal praktijkgevallen de uitkomsten van de onderzoeken en de impact op de controleaanpak besproken. Tot slot worden de belangrijkste ervaringen uit de praktijk en randvoorwaarden samengevat.

General IT controls

De betrouwbaarheid van een IT-systeem wordt beheerst door computercontroles met een algemeen karakter (de general IT controls of algemene computercontroles) en computercontroles die zich richten op de betrouwbare werking van een specifieke applicatie (de application controls of toepassingscontroles) ([Munc95]). Bij voortschrijdende automatisering worden onder meer uit efficiëntieoogpunt in toenemende mate controles in de applicatie geïmplementeerd. Om ervoor te zorgen dat deze application controls bij voortduring effectief zijn, worden hogere eisen gesteld aan de general IT controls. Immers, de organisatie moet er zeker van zijn dat getes-te en geaccepteerde toepassingsprogrammatuur daadwerkelijk is geïmplementeerd en in continuïteit ongewijzigd blijft. De general IT controls dienen derhalve te voldoen aan de eisen die vanuit de organisatie worden gesteld.

Op basis van de aandachtsgebieden van de general IT controls worden de volgende belangrijke beheersgebieden onderscheiden met de vermelding van de doelstellingen voor de te nemen maatregelen:
* *beleid en management*. Deze maatregelen zijn gericht op het vaststellen dat het beleid van een organisatie en de managementprocedures effectief zijn in de beheersing van de automatiseringsfunctie;
* *informatiebeveiliging*. Hieronder vallen maatregelen die zijn gericht op de beveiliging van de (kritische) informatie. De logische toegangsbeveiliging vormt hier een onderdeel van. In toenemende mate wordt informatie opgenomen in geïntegreerde informatiesystemen zodat gezamenlijk gebruik van gegevens mogelijk is. Om de in de administratieve organisatie opgenomen functiescheidingen ook in deze informatiesystemen te kunnen realiseren wordt gebruikgemaakt van logische toegangsbeveiliging;
* *fysieke beveiliging*. Deze maatregelen zijn gericht op het minimaliseren van het risico van bewust of per ongeluk veroorzaken van schade aan of diefstal van bijvoorbeeld computerapparatuur, programmatuur en gegevens. Tevens spelen omgevingsomstandigheden zoals de stroomvoorziening een rol;
* *continuïteit*. De maatregelen omtrent continuïteit zijn gericht op het bewerkstelligen van een ongestoorde voortgang van de gegevensverwerking;
* *change management*. Het betreft maatregelen inzake technische en organisatorische veranderingen die binnen een organisatie plaatsvinden. Change management is het proces van evalueren, plannen en coördineren van de implementatie en van de wijzigingen in de informatiesystemen en de verwerkingsorganisatie. Omdat elke verandering in principe bedreigingen met zich meebrengt, is het belangrijk maatregelen te nemen;
* *systeemontwikkeling/aankoop van systemen*. Deze maatregelen zijn gericht op het zeker stellen dat ontwikkelde of standaardsystemen en wijzigingen in programmatuur geautoriseerd, getest, gedocumenteerd en gerealiseerd worden. Dit om ervoor te zorgen dat de systemen voldoen aan de wensen van de gebruikers;
* *beoordeling van automatisering*. Organisaties zijn voortdurend in beweging. Om te controleren of de huidige automatiseringssituatie nog steeds voldoet aan de eisen en wensen van de organisatie, moeten maatregelen zijn getroffen die waarborgen dat de automatisering periodiek wordt beoordeeld.

Door het niveau van de general IT controls op een consistente en systematische wijze te meten en de gegevens

ervan in een database te verzamelen, is het mogelijk benchmarks samen te stellen.

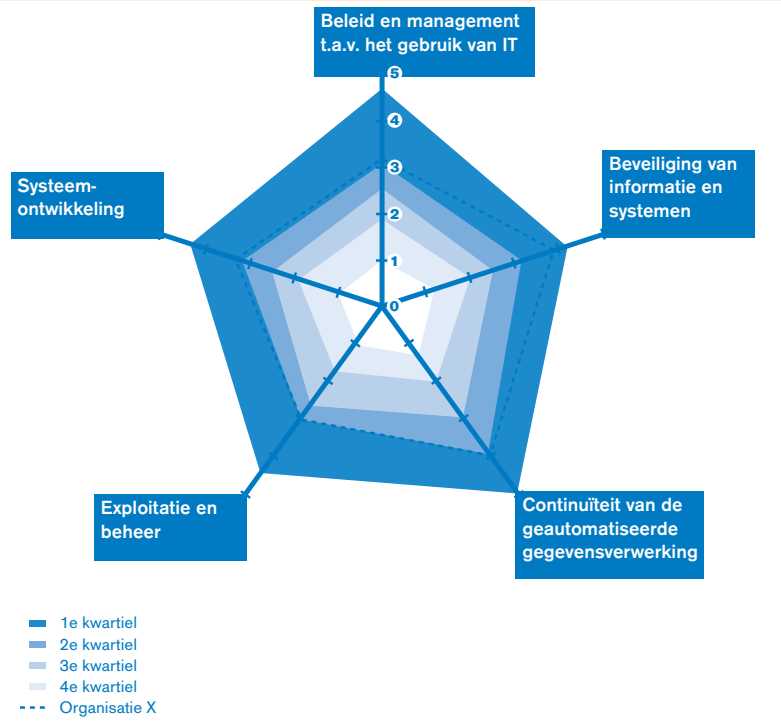
Benchmarking van ICT-controls

KPMG heeft een benchmarkingmethode ontwikkeld die een organisatie de gelegenheid geeft haar general IT controls te toetsen aan die van vergelijkbare organisaties of de 'best practices' binnen en buiten de branche. De informatie uit deze vergelijking stelt de organisatie in staat de beheersingsmaatregelen rond de toepassing van IT te verbeteren en risico's effectiever te beheersen. Het product IT Benchmarking wordt wereldwijd in diverse landen door KPMG bij haar klanten ingezet.

In de benchmarkingonderzoeken worden de aandachtsgebieden van general IT controls onderzocht door vragen te stellen en controlebewijs te verzamelen naar het gebruik van beheersmaatregelen. De vragen zijn gebaseerd op een groeimodel. Hierbij worden vijf afzonderlijke fasen gedefinieerd. Op deze vragen kan een score worden gegeven van 1 tot en met 5. De score op de vragen wordt geverifieerd door de onderzoeker. De verificatie geschiedt door te vragen naar bewijzen voor de gegeven antwoorden. De achterliggende gedachte van de score 1 tot en met 5 is:

1 De organisatie heeft geen maatregelen getroffen.
2 De organisatie heeft informele maatregelen getroffen.
3 De organisatie heeft formele maatregelen getroffen.
4 De organisatie beheerst de maatregelen en stuurt.
5 Er is een evaluatiecyclus om de maatregelen bij en af te stellen op de wensen uit de organisatie (proactief).

Figuur 1. Voorbeeld benchmark IT-beheersmaatregelen.



Voor de presentatie van de benchmarkingresultaten wordt gebruikgemaakt van zogenaamde spinnenwebgrafieken. Een voorbeeld hiervan wordt weergegeven in figuur 1.

In figuur 1 geeft de stippellijn de score op een schaal van 1 tot en met 5 van organisatie X weer. Hierbij geeft de score 1 aan dat geen beheersmaatregelen zijn getroffen en de score 5 geeft aan dat proactief met de getroffen beheersmaatregelen wordt omgegaan binnen de organisatie. De scores van de organisaties waarmee de organisatie X is vergeleken, zijn weergegeven in kwartielen (25-procentsintervallen). Op bijvoorbeeld het onderdeel Systeemontwikkeling scoort de organisatie X hoger dan (meer dan) 75% van de andere organisaties.

De data die als vergelijkingsmateriaal wordt gebruikt, komt voort uit 1800 internationale benchmarkingonderzoeken die de afgelopen jaren zijn uitgevoerd. De onderzoeken zijn uitgevoerd bij bedrijven uit de volgende branches: banken, verzekeringen, dienstverlening, handel, overheid, transport, olie en metalen, chemische industrie, elektronica, technische industrie, foodindustrie en bouw.

Praktijkcases

De cases richten zich op de verschillende wijzen waarop ten behoeve van het management van organisaties en de accountant aandacht wordt besteed aan de general IT controls. Tevens wordt ingegaan op hetgeen het management en/of de accountant heeft gedaan met het gemeten niveau van de general IT controls.

Casus 1: Organisatie X met meerdere businessunits

Organisatie X bestaat uit meerdere businessunits die verspreid door het land zijn gevestigd. De organisatie is in sterke mate afhankelijk van IT. De betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking is derhalve van groot belang. De IT is decentraal georganiseerd. Elke businessunit beschikt over een IT-afdeling van beperkte omvang. Deze afdelingen houden zich met name bezig met de exploitatie en het beheer van de lokale IT-infrastructuur. Het IT-beleid en realisatie van dit beleid door middel van diverse IT-projecten vindt centraal vanuit het hoofdkantoor plaats.

Drie jaar geleden is een eerste onderzoek uitgevoerd naar het niveau van de general IT controls. De belangrijkste conclusie die naar aanleiding van het benchmarkingonderzoek naar voren kwam, was dat het niveau van de general IT controls per businessunit sterk varieerde en dat het niveau in zijn algemeenheid volgens de benchmark laag was. Met name op het gebied van logische toegangsbeveiliging, change management, fysieke toegangsbeveiliging en contingency management was het niveau van de genomen maatregelen onvoldoende om mogelijke risico's af te dekken. Als gevolg hiervan hadden zich in bepaalde businessunits verschillende incidenten voorgedaan. Voorbeelden van risico's waren:

* Gebruikers beschikten over dusdanige bevoegdheden dat functiescheidingen werden doorbroken.
* Wijzigingen op applicaties werden direct in de productieomgeving aangebracht zonder dat deze goed waren getest.

* Onbevoegden hadden toegang tot kritische ruimten.
* Er waren onvoldoende mogelijkheden om tijdig te kunnen uitwijken.

Een andere conclusie was dat tussen businessunits onderling weinig of geen afstemming plaatsvond inzake het voorstellen en realiseren van verbeteringen van de aanwezige maatregelen. De businessunit waar zich een brand had voorgedaan in de computerruimte had een calamiteitenplan opgesteld. Tevens was een contract afgesloten voor IT-uitwijk. Een andere unit had als enige een procedure opgesteld waarin werd aangegeven dat wijzigingen pas nadat deze door gebruikers waren getest in productie mochten worden genomen. Daarnaast was er een testomgeving ingericht.

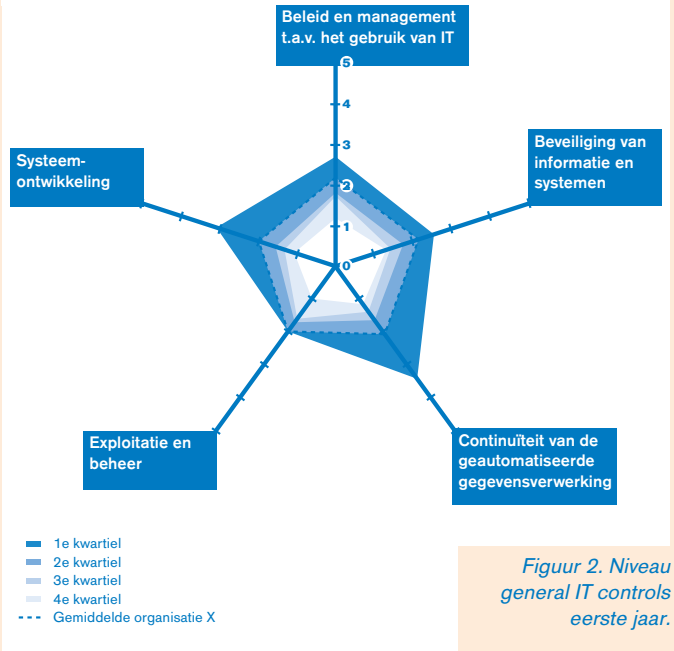
Als gevolg van het ontbreken van onderlinge afstemming werd binnen de businessunits geen gebruik gemaakt van de kennis die al in de organisatie op de verschillende general IT controls-gebieden aanwezig was. Hierdoor werden (veel) resources besteed aan werkzaamheden die al eerder binnen andere businessunits waren uitgevoerd.

Op basis van de bevindingen heeft de directie van deze organisatie besloten het niveau van de general IT controls voor de gehele organisatie op hetzelfde niveau (de baseline) te brengen. Uitgangspunt hierbij was dat gebruik diende te worden gemaakt van de kennis en maatregelen die al op de verschillende aandachtsgebieden binnen de afzonderlijke units aanwezig waren. Besloten is hiervoor een organisatiebreed project op te zetten en de verbeteringen door te voeren aan de hand van de Code voor Informatiebeveiliging. De Code voor Informatiebeveiliging is een naslagdocument voor bedrijven en instellingen voor het opzetten, implementeren en onderhouden van informatiebeveiliging ([NEN94]). Door de organisatie is een informatiebeveiligingsplan opgesteld. Hierin zijn onder andere de normen aangegeven waaraan elke businessunit moet voldoen. Op elk van de units is iemand verantwoordelijk gesteld om uitvoering te geven aan het informatiebeveiligingsplan. Jaarlijks wordt door de IT-auditor een meting gedaan in hoeverre de afzonderlijke businessunits voldoen aan de normen. Tevens worden de afzonderlijke units met elkaar vergeleken en worden de resultaten gebenchmarkt met soortgelijke organisaties. De resultaten worden rechtstreeks aan de directie gerapporteerd. Het management van de businessunits dient zich bij het afwijken van de norm (zowel bij positieve als negatieve afwijking) te verantwoorden bij de directie.

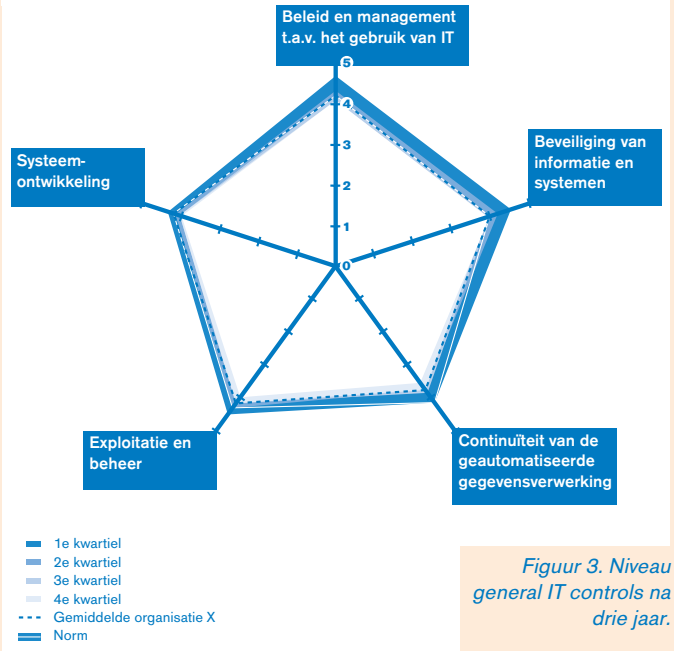
> Het gebruik van benchmarks kan als een toegevoegde waarde aan de audit worden gezien.

De accountant heeft ten behoeve van de jaarrekeningcontrole op basis van de rapportage per businessunit een controleprogramma opgesteld. De controleaanpak varieerde sterk per unit. Bij die units waar het niveau van de general IT controls erg laag was, is uitgegaan van een controleaanpak met een gegevensgericht karakter. Bij een tweetal units waren de general IT controls van een voldoende niveau. Bij deze units is uitgegaan van een systeemgerichte aanpak waarbij gesteund is op informatie verkregen uit de verschillende geautomatiseerde systemen. Mede als gevolg van het verschil in het niveau van de general IT controls varieerde de tijd die benodigd was voor de jaarrekeningcontrole sterk per unit.

Toelichting figuur 2 en 3
Bij deze organisatie is er bewust voor gekozen de bevindingen grafisch te rapporteren. In één oogopslag is het zichtbaar hoe de general IT controls van de verschillen-



Figuur 2. Niveau general IT controls eerste jaar.



Figuur 3. Niveau general IT controls na drie jaar.

de businessunits zich tot elkaar verhouden (zie figuur 2). Het gemiddelde niveau van de general IT controls van de verschillende units is relatief laag en varieert tussen een score 1 en 2. Uit figuur 2 is op te maken dat verschillende units op een aantal punten relatief hoog scoren ten opzichte van de andere units. Voor het management van de gebenchmarkte units verschaft deze vorm van presenteren van resultaten meer helderheid dan omvangrijke rapportages. Een voordeel is eveneens dat naast afwijkingen in negatieve zin ook afwijkingen in positieve zin zijn af te lezen.
De situatie na drie jaar is in figuur 3 weergegeven. Hierbij geeft de witte lijn de normscore aan die door de organisatie zelf is vastgesteld. Met behulp van het benchmarkingonderzoek is ook te zien of de opgezette en uitgevoerde verbetertrajecten daadwerkelijk tot resultaat hebben geleid. Tevens is vast te stellen of de gestelde normen zijn gerealiseerd.
Drie jaar verder liggen, na de realisatie van de verbetertrajecten, de general IT controls op een vrijwel gelijk (hoog) niveau. De verschillende units voldoen nagenoeg aan de normscore. Het verschil in kwaliteitsniveau van de general IT controls dat in het eerste jaar aanwezig was, is verdwenen (zie de geringe spreiding van de kwartielen). Zowel de IT-organisatie als de gebruikersorganisatie is van mening dat hierdoor de beheersing van de IT een hoger volwassenheidsniveau heeft gekregen. In plaats van reactief wordt proactief opgetreden. Gebruikers vinden het normaal dat ze alleen die systeembevoegdheid hebben die uit het oogpunt van hun functie noodzakelijk is. Het komt nagenoeg niet meer voor dat gebruikers als gevolg van niet-geteste systeemwijzigingen niet meer met het systeem kunnen werken. Door een goed uitwijkdraaiboek was het mogelijk om na vijftien uur weer operationeel te zijn na een waterlekkage in een lokale computerruimte. De organisatie is minder kwetsbaar geworden voor incidenten en als er zich incidenten voordoen dan is duidelijk hoe en wanneer hierop in te spelen. De laatste drie jaar is deze organisatie in toenemende mate afhankelijk geworden van IT. De organisatie kan het zich niet langer veroorloven te werken zonder een betrouwbare en continu beschikbare IT-infrastructuur.

De accountant heeft op basis van de voortgang en stroomlijning die heeft plaatsgevonden ten aanzien van de general IT controls de controleprogramma's van de verschillende units op elkaar aangepast. Overgegaan is van een gegevensgerichte naar een hoofdzakelijk systeemgerichte controleaanpak. Geconcludeerd wordt dat mede door het verbeteren van de general IT controls de betrouwbaarheid en continuïteit van de geautomatiseerde gegevensverwerking sterk is verbeterd en de jaarrekeningcontrole is gestroomlijnd.

Casus 2: Organisatie Y, een productieonderneming
Organisatie Y is een middelgrote productieonderneming. De organisatie is gevestigd op één locatie en is in sterke mate afhankelijk van IT. De IT-afdeling bestaat uit één medewerker. De systeemontwikkeling en exploitatie en beheer van de IT-infrastructuur zijn uitbesteed aan een derde partij.

De keuze voor een derde partij was twee jaar geleden gemaakt, mede naar aanleiding van de resultaten van een benchmarkingonderzoek naar het niveau van de general IT controls bij deze organisatie. De belangrijkste conclusie van het onderzoek was dat het ontwikkelen van IT-beleid een sterk punt van de organisatie was. Het beheer van informatiesystemen daarentegen vormde duidelijk een aandachtsgebied. Mede op basis van deze conclusie is enkele jaren geleden dan ook door organisatie Y besloten dat IT niet tot de kerntaken van de organisatie behoorde en dat de systeemontwikkeling en exploitatie en beheer van de IT-infrastructuur zouden worden geoutsourced. Het niveau van de general IT controls van organisatie Y was hierdoor mede afhankelijk van het bij de outsourcer getroffen maatregelenniveau.

Een adequate inrichting van de logische toegangsbeveiliging was binnen de organisatie een aandachtsgebied. Het beleid was erop gericht dat medewerkers alleen die systeembevoegdheden werden toegekend die zij uit hoofde van hun functie nodig hadden. De organisatie was ervan overtuigd dat door het nemen van eigen maatregelen gecombineerd met de maatregelen genomen bij de outsourcer de general IT controls van een hoog niveau waren. Zij had echter geen inzicht in de door de outsourcer genomen maatregelen. Zo was onduidelijk of andere klanten van de outsourcer toegang hadden tot de infrastructuur van organisatie Y. Tevens was het niet duidelijk welke continuïteitsmaatregelen er door de outsourcer waren genomen om te voorkomen dat de organisatie langere tijd zonder IT-infrastructuur zou komen te zitten. Daarnaast was er geen goed zicht op het changemanagementproces. Er was geen service level agreement (SLA) opgesteld waarin dergelijke onderwerpen aan de orde kwamen. Organisatie Y ging ervan uit dat de outsourcer dusdanig professioneel was dat deze passende maatregelen had genomen.

In overleg met het management van de organisatie, de accountant en de outsourcer heeft de IT-auditor een benchmarkingonderzoek uitgevoerd. Uit dit onderzoek kwam naar voren dat het niveau van de general IT controls op belangrijke punten onvoldoende was. In de benchmark scoorde de outsourcer laag ten opzichte van andere vergelijkbare organisaties. Het controleplan van de accountant is hierop aangepast doordat aanvullende controles zijn uitgevoerd. In onderling overleg heeft de IT-auditor een normenset opgesteld voor de outsourcer. Aan de hand van deze normenset is een verbetertraject door de outsourcer uitgevoerd. Nu twee jaar later is het verbetertraject afgerond. De IT-auditor controleert periodiek de naleving van de normenset. Dit jaar heeft dit geleid tot het afgeven van een Third Party Mededeling (TPM). Door de accountant wordt ten behoeve van de jaarrekeningcontrole gesteund op deze TPM.

Casus 3: Organisatie U, een dienstverlener
Organisatie U is een relatief grote handelsonderneming. De organisatie is gevestigd op één locatie en is in sterke mate afhankelijk van IT. De organisatie verleent diensten voor aangesloten leden. Deze zijn geografisch verspreid over Nederland. De IT-afdeling bestaat uit twintig medewerkers. Hiervan houdt ongeveer de helft zich bezig met systeemontwikkelingsactiviteiten.

Voor deze organisatie is op verzoek van de accountants een benchmarkingonderzoek uitgevoerd naar de general IT controls. Dit onderzoek heeft plaatsgevonden in combinatie met een specifiek onderzoek naar de inrichting en beheersing van de AS/400. Voorafgaand aan het onderzoek is de aanpak eerst afgestemd met de organisatie. Op deze wijze was helder wat het object van onderzoek was en op welke wijze de beheersorganisatie in kaart zou worden gebracht.

De benodigde gegevens zijn in samenwerking met de organisatie in kaart gebracht en verzameld. Vervolgens zijn de gegevens getoetst, afgestemd en verwerkt met behulp van het benchmarking-tool. Zoals eerder aangegeven is een groot voordeel van het gebruik van het benchmarking-tool dat informatie over beheersing van IT in grafieken wordt weergegeven. Mede gezien de vorm van de presentatie van de gegevens was bij de terugkoppeling van de resultaten naast IT-medewerkers ook de directie aanwezig. De resultaten zijn door zowel de IT-auditor als de accountant toegelicht aan de hand van de benchmarkingpresentatie. De bevindingen van het AS/400-onderzoek waren hierin opgenomen. Hierdoor kon de directie zonder diepgaande AS/400-kennis de mate van beheersing zien en konden de aangetroffen aandachtsgebieden op een juiste wijze worden overgebracht.

Het belangrijkste resultaat van het onderzoek was dat het niveau van de aangetroffen beheersmaatregelen gemiddeld scoorde ten opzichte van andere soortgelijke organisaties (hardware-infrastructuren). Gezien het bewustzijn van de organisatie inzake de risico's die de inzet van IT met zich meebrengt en de investeringen die in IT worden gepleegd, kon de organisatie zich duidelijk hierin terugvinden. Deze acceptatie vormde de voornaamste reden om de vastgestelde aandachtsgebieden naar voren te brengen.

Een belangrijk aandachtspunt vormde het verder verbeteren van de maatregelen op het gebied van continuïteit. De organisatie is sterk afhankelijk van de geautomatiseerde gegevensverwerking. De huidige getroffen maatregelen waren beperkt en informeel van aard en konden derhalve onvoldoende waarborgen bieden. Het risico is aanwezig dat de bedrijfsprocessen tijdelijk niet meer kunnen worden voortgezet. Voor zowel de automatisering als de bedrijfsprocessen was het van belang dat er een calamiteitenplan werd opgezet. Een ander aandachtspunt vormde de change-managementprocedure. De impact van wijzigingen werd niet vastgesteld en een wijziging werd niet op een beheerste wijze in de organisatie (test-, acceptatie- en overdrachtsprocedure) ingebed. Als gevolg hiervan werden gebruikers in de praktijk nog wel eens 'verrast' met een doorgevoerde wijziging, wat (tijdelijk) leidde tot extra klachten. Tevens bleek uit praktijkvoorbeelden dat de integriteit van de database niet was gewaarborgd. Een ander belangrijk punt was dat de belangrijkste informatiesystemen nogal eens performanceproblemen kenden. De traagheid van het systeem leidde tot klachten van gebruikers en een grote belasting van de IT-afdeling alsmede tot fouten van gebruikers. In de communicatie met de leden van de organisatie ontstonden problemen omdat antwoorden niet altijd direct konden worden gegeven door de trage werking van het informatiesysteem.

Met name een onvoldoende beheerst change-managementproces is in het kader van de jaarrekeningcontrole van belang, omdat wijzigingen van invloed kunnen zijn op de werking van de informatiesystemen en daarmee op de betrouwbaarheid van gegevens. Dit kan leiden tot het uitvoeren van aanvullende controles. Het gebruik van de grafieken, gegenereerd door het benchmarking-tool, heeft meegeholpen om ten behoeve van de organisatie de belangrijkste verbetergebieden helder te krijgen. De punten zijn door de accountant tegen de organisatie aangehouden met de vraag welke actie wordt ondernomen.

> Een groot voordeel van het gebruik van het benchmarking-tool is dat informatie in grafieken wordt weergegeven.

De acceptatie van de resultaten heeft ertoe geleid dat de organisatie acties, voorzien van een realisatiedatum, heeft opgezet. Op basis hiervan kunnen de organisatie zelf en de accountants sturen op voortgang en realisatie. Voor zowel de activiteiten in het kader van de jaarrekeningcontrole als voor de organisatie zelf heeft een IT Controls Benchmarking-onderzoek ertoe geleid dat de aandachtsgebieden in kaart zijn gebracht en dat verbeteracties duidelijk kunnen worden geadresseerd. Het toepassen van benchmarking heeft als voordeel dat de resultaten in een beter te begrijpen vorm aan de diverse betrokkenen van de organisatie kunnen worden gepresenteerd, ook indien niet over diepgaande IT-kennis wordt beschikt.

Casus 4: Organisatie P, werkzaam in bouw en constructie

Organisatie P bestaat uit meerdere werkmaatschappijen die verspreid door het land zijn gevestigd. De organisatie is op onderdelen afhankelijk van IT maar deze afhankelijkheid neemt in snel tempo toe. De IT is decentraal georganiseerd. Elke businessunit beschikt over een IT-afdeling van beperkte omvang. Deels werken werkmaatschappijen met elkaar samen om invulling te geven aan de IT-functie. Het IT-beleid en realisatie van dit beleid door middel van diverse IT-projecten vindt decentraal plaats. Centraal is er sprake van beperkte coördinatie.

Op verzoek van de controlerend accountants is een benchmarkingonderzoek uitgevoerd naar de general IT controls bij een aantal werkmaatschappijen. De selectie van de werkmaatschappijen heeft in samenwerking met de centrale organisatie plaatsgevonden. Doordat van de organisatie meerdere werkmaatschappijen werden onderzocht, was het mogelijk naast vergelijking met andere soortgelijke organisaties ook een interne vergelijking te maken.

De afhankelijkheid van IT is binnen de organisatie pas de afgelopen jaren toegenomen. Dit heeft in de praktijk tot gevolg dat de inrichting van de beheersing van IT nog volop in ontwikkeling is. Gezien de toename van de IT-ontwikkelingen is ook deze organisatie in aanraking met IT-audit gekomen. De doelstelling en de toegevoegde

waarde van een IT-audit waren binnen de organisatie relatief onbekend. Het nut van de beoordeling van de general IT controls was voor de organisatie dan ook nog niet helder. Randvoorwaarde voor het meewerken van de organisatie aan het IT Benchmarking-onderzoek was dat de resultaten daadwerkelijk aanwijzingen voor verbeteringsgebieden konden opleveren. Om te komen tot een succesvolle samenwerking was het van kritiek belang dat de IT-auditors samen met de accountants vaststelden op basis van welke strategie de organisatie diende te worden benaderd en wat de specifieke aandachtsgebieden waren. De aanpak is voorafgaand aan het uit te voeren onderzoek individueel met de diverse werkmaatschappijen afgestemd. Door deze zorgvuldige afstemming was voor zowel de organisatie als de accountant helder welke resultaten het onderzoek zou moeten opleveren. De praktijk leert dat het creëren van acceptatie vooraf leidt tot een verhoging van de kwaliteit van de verkregen informatie en tot het daadwerkelijk initiëren van verbeteracties.

Voorafgaand aan het onderzoek was de verwachting dat de afhankelijkheid van IT niet erg groot was. Op basis van het uitgevoerde onderzoek is vastgesteld dat de afhankelijkheid reeds behoorlijk groot was en, gezien de ontwikkelingen, sterk toenam. In het algemeen werd in de benchmark door de werkmaatschappijen ten minste gemiddeld gescoord. Hieruit kon worden geconcludeerd dat het niveau van de general IT controls zich verhoudt tot datgene wat bij vergelijkbare bedrijven wordt aangetroffen. Een verrassende bevinding was dat het niveau van de beheersmaatregelen van de onderzochte werkmaatschappijen grotendeels overeenkwam. De verwachting van de werkmaatschappijen was dat er grote onderlinge verschillen bestonden.

Benchmarking van general IT controls biedt een relatief eenvoudige en snelle manier om inzicht te krijgen in de kwaliteit van complexe omgevingen.

Belangrijk aandachtspunt vormde de vaak vrij informeel ingerichte beheersing van IT. Hierdoor was het niet mogelijk aantoonbaar vast te stellen dat de betrouwbaarheid en de continuïteit van de geautomatiseerde gegevensverwerking voldoende waren gewaarborgd. Een verdere professionalisering was, gezien de toenemende afhankelijkheid, van belang en dit is ook door de werkmaatschappijen onderschreven. In de huidige situatie waren de taken en verantwoordelijkheden sterk geconcentreerd bij de IT-medewerkers. Er was slechts een beperkt toezicht op de activiteiten van de IT-medewerkers. Een ander belangrijk resultaat van het onderzoek was het feit dat het management meer doordrongen raakte van de risico's ten aanzien van het gebruik van IT en het gewenste niveau van te treffen beheersmaatregelen. Het onderzoek zelf en het verkregen inzicht werden door de werkmaatschappijen als een zeer waardevolle exercitie aangeduid.

Op basis van de uitgevoerde onderzoeken is helder in kaart gebracht wat de status is van het huidige niveau van de beheersmaatregelen. Voor zowel de accountant als de organisatie is helder dat een verdere professionalisering van de IT-organisatie dient plaats te vinden alvorens volledig kan worden gesteund op de kwaliteit van de in informatiesystemen verankerde controlemaatregelen. Een bijkomend resultaat van het onderzoek is dat de organisatie meer inzicht heeft verkregen in de risico's ten aanzien van het gebruik van IT en de wijze waarop de risico's zijn af te dekken. Het was ook niet moeilijk de organisatie ervan te overtuigen dat op bepaalde punten verbeteringen nodig waren. Organisatie P was sterk gedreven om 'goed' te scoren ten opzichte van de benchmark. Deze houding heeft ertoe geleid dat de organisatie de aanwezige risico's wilde afdekken en de maatregelen zo spoedig mogelijk wilde implementeren. Tevens was de organisatie meer bereid om de toekomstige ontwikkelingen te bespreken en daarbij de kennis en ervaring van de accountant en IT-auditor te betrekken. De case geeft aan dat naar aanleiding van het uitvoeren van een IT Benchmarking-onderzoek de communicatie tussen organisatie, IT-auditors en accountants sterk is verbeterd en het mogelijk wordt sneller en beter inzicht te krijgen in de aandachtsgebieden. Deze aspecten hebben sterk bijgedragen aan de planning en de efficiency van de uitvoering van de audits.

Samenvatting belangrijkste ervaringen en randvoorwaarden uit de praktijk

De cases geven enkele voorbeelden uit de praktijk weer waarin een aantal belangrijke ervaringen en leermomenten is opgenomen. Op basis van de tot nu toe wereldwijd uitgevoerde IT Benchmarking-onderzoeken kunnen de belangrijkste ervaringen als volgt worden samengevat:

* De methode biedt een relatief eenvoudige en snelle manier om inzicht te krijgen in de kwaliteit van complexe omgevingen.
* De benchmark signaleert de afwijkingen ten opzichte van andere organisaties, wat voor de gebenchmarkte organisatie punten voor discussie oplevert. Tevens levert de uitgevoerde benchmark aandachtspunten voor de auditaanpak maar ook voor de management letter. Deze punten worden in het algemeen sterk gewaardeerd door het management van de betreffende organisatie.
* De uitvoering en de presentatie van de resultaten spreken het management duidelijk aan. De organisatie wordt niet alleen beoordeeld maar krijgt ook voldoende punten aangereikt waarop daadwerkelijk actie kan worden ondernomen. De IT-organisatie van de organisatie is hiermee duidelijk geholpen, mede doordat het bewustzijn van het management is vergroot.
* De interactie tussen de te beoordelen organisaties, de IT-auditors en de accountants is vergroot, wat leidt tot een beter wederzijds begrip en acceptatie. Hierdoor is de toegevoegde waarde van IT-audits vergroot en duidelijker zichtbaar. De discussie over de tekortkomingen heeft plaatsgemaakt voor de discussie over de te verbeteren gebieden.
* Een IT Benchmarking-onderzoek kan nooit een volledig detail/diepteonderzoek vervangen omdat de diverse aandachtsgebieden in kaart worden gebracht en het totaalbeeld het resultaat is. Op basis van de vastgestelde

aandachtsgebieden kan door de organisatie of door de IT-auditor nader onderzoek worden verricht. Een andere mogelijkheid is bijvoorbeeld om op basis van de resultaten van het vorige jaar, meer aandacht te besteden aan een aandachtsgebied om resultaten op een gedetailleerder niveau te genereren.

* Alleen de vergelijking met andere organisaties kan niet dienen als audit evidence. Er dient ook zelfstandig onderzoek (met behulp van het IT Benchmarking-tool) plaats te vinden door een IT-auditor. De normen van de auditor en de eisen gesteld door de organisatie bepalen de aandachtsgebieden, niet een score lager of hoger dan andere organisaties.

De ervaringen geven aan dat het gebruik van IT Benchmarking voor de general IT controls veel voordelen oplevert. Om van de voordelen (blijvend) te kunnen profiteren zijn de volgende belangrijke randvoorwaarden gesteld:

* Het uitvoeren van IT Benchmarking is geen eenmalige actie maar een continu proces. De vergelijking met andere organisaties en de aangetroffen situatie bij een organisatie is een momentopname. Organisaties zijn continu in beweging en nemen jaarlijks diverse beslissingen, zoals het outsourcen van IT. De kwaliteit van de beheersmaatregelen kan derhalve veranderen. Om terecht te kunnen steunen op de beheersing van IT is het van belang periodiek de ontwikkelingen met de organisatie door te nemen en de kwaliteit van de general IT controls te meten.
* Het uitvoeren van IT Benchmarking vereist voldoende kennis over het onderwerp en ervaring met benchmarking. Het meten en vergelijken van organisaties maakt de afwijkingen duidelijk zichtbaar. Het helder aan het licht komen van afwijkingen leidt veelal tot heftige reacties van organisaties en accountants. Het is van belang dat de IT-auditor hiermee op een juiste wijze kan omgaan, zodat de aanwezige 'emoties' kunnen worden omgezet in acceptatie van de resultaten en het toewerken naar verbeteringen.
* Er moet met een minimaal aantal organisaties worden vergeleken (uitgangspunt is: minimum van vijf vergelijkbare organisaties, bijvoorbeeld geselecteerd op branche en omvang IT-organisatie). Een grote en voldoende gesegmenteerde database is derhalve van belang.
* De scores van vergelijkbare organisaties zijn geen norm. Op basis van een nadere analyse dient te worden vastgesteld wat de daadwerkelijke knelpunten zijn.

Conclusie

In dit artikel is de ervaring in de praktijk met het benchmarken van de general IT controls uiteengezet. Tevens is de invloed op de activiteiten in het kader van de controleaanpak behandeld. De methodiek IT Benchmarking vervult de behoefte van organisaties ten aanzien van vergelijkingsgegevens en biedt een grafische weergave van de positie ten opzichte van andere organisaties. In het kader van de jaarrekeningcontrole levert het benchmarken van de general IT controls de accountant het volgende op:

* inzicht in risico's en waarborgen ten aanzien van betrouwbaarheid en continuïteit van IT;
* inzicht in de wijze waarop wordt omgegaan met IT (grip op automatiseringsactiviteiten);
* inzicht in de omgang met gestelde wetgeving en/of Memorandum DNB.

Voor het analyseren van de uitkomsten van benchmarking moeten de resultaten kunnen worden geïnterpreteerd en geëvalueerd. In het artikel is aangegeven dat kennis over (de general IT controls) en ervaring met benchmarking een belangrijke rol spelen. Ook is aangegeven dat het belangrijk is naast benchmarks de normen van de IT-auditor tegen een organisatie aan te leggen.

Literatuur

[Boer97]
J.C. de Boer en J.R.M. Vandecasteele, *De EDP-auditor en de veranderende ICT-organisatie*, Compact 1997/4.

[Camp89]
R.C. Camp, *Benchmarking: The search for Industry Best Practices That Lead to Superior Performance*, Milwaukee WI, Quality Press, 1989.

[Donk96]
J.A.M. Donkers en E.R. van Sommeren, *Benchmarking, een hulpmiddel voor de EDP-auditor?*, Compact 1996/2.

[Munc95]
W.A. de Munck, *Informatietechnologie als beoordelingsobject in de hedendaagse controlebenadering*, Compact 1995/3.

[NEN94]
Code voor informatiebeveiliging, Een leidraad voor beleid en implementatie, Nederlands Normalisatie-instituut, 1994.

[Pryo89]
L.S. Pryor, *Benchmarking: A Self-Improvement Strategy*, The Journal of Business Strategy, November/December 1989.

[Somm97]
E.R van Sommeren, J.C. de Boer en J.A.M. Donkers, *Benchmarking van Informatietechnologie*, Automatisering Gids, oktober 1997.

Drs. J.C. de Boer RE
is als manager werkzaam bij KPMG Information Risk Management. Zijn aandachtsgebied ligt op het gebied van benchmarking en management van IT. Hij is betrokken bij audit- en begeleidingsopdrachten van IT-organisaties en is verantwoordelijk voor IT Benchmarking in Nederland.

Mw. ir. E.R. van Sommeren RE
is als manager werkzaam bij KPMG Information Risk Management. Belangrijke aandachtsgebieden in haar werk zijn de inrichting en beheersing van de informatievoorziening binnen organisaties en het begeleiden van organisaties bij het verbeteren van de processen. Benchmarking van IT is één van haar aandachtsgebieden waarvoor zij productontwikkeling heeft uitgevoerd.