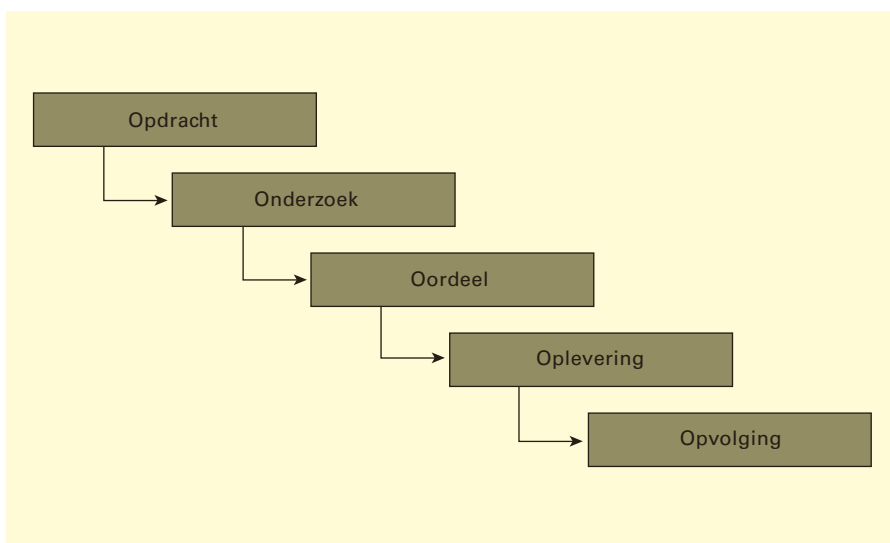


Goede voorbereiding en opdrachtformulering onontbeerlijk

Bijdrage ICT aan bedrijfsresultaat helder met auditing

ICT speelt binnen organisaties een steeds belangrijkere rol doordat bedrijfsprocessen in toenemende mate worden geautomatiseerd. Om de kwaliteit van die processen te kunnen borgen is het van belang regelmatig de procesondersteunende automatiseringsvoorzieningen te (laten) toetsen of beoordelen. Het uitvoeren van een audit is een goede manier om zekerheid te verschaffen óf om onzekerheid weg te nemen over de bijdrage die de ICT aan de bedrijfsvoering levert. Voorwaarde voor succes is echter wel een goede voorbereiding en opdrachtformulering.



Afbeelding 1. Globale fasering van een audit.

Om zicht op de ICT binnen organisaties te krijgen en te houden is een audit een belangrijk en waardevol instrument. Zowel voor opdrachtgevers als uitvoerders is het van groot belang bewust om te gaan met de verschillende verschijningsvormen waarin audits voor

kunnen komen. Een goede voorbereiding en opdrachtformulering van een ICT-audit is dan ook onontbeerlijk.

Auditfasen

Bij een audit zijn in grote lijnen een aantal fasen te onderkennen (zie af-

beelding 1). Het voorbereiden van een audittraject gebeurt door per fase stil te staan bij een aantal aandachtspunten die bepalend zijn voor de kwaliteit van het eindresultaat. In dit artikel gaan we, na een korte toelichting op de fasering, in op een tweetal aandachtspunten. Dit zijn de vorm van de audit en de keuze voor het tijdstip om een audit uit te voeren.

Aan de hand van een analyse per fase kan de opdrachtgever de verwachtingen van het traject vooraf expliciet maken en hiermee de basis leggen voor een goed eindresultaat. Bij het formuleren van de *opdracht* staan drie dingen centraal: het afbakenen van de scope van de opdracht, het maken van een keuze over de vorm van de audit en het bepalen van een normenkader. Speciaal aandachtspunt bij de bepaling van de scope van een audit is het niveau waarop het onderzoek wordt uitgevoerd. In het geval van een ICT-audit speelt bijvoorbeeld de vraag of deze gericht is op de informatie, de informatievoorziening of de informatiesystemen.

Als voorbereiding op de uitvoering van het *onderzoek* komt het proces en de methode van uitvoering aan de orde. Hierin spelen praktische zaken als interviews en documentatie een rol, waarbij het met name gaat om vooraf na te denken over welke informatie beschikbaar is en hoe deze ter beschikking kan worden gesteld. Het aantal interviews, de doorlooptijd en de aard van het bronmateriaal zijn in belangrijke mate bepalend voor de diepgang van het onderzoek.

Volgende stap is het *oordeel*. De literatuur beschrijft een audit als een proces waarin een deskundig, onpartijdig en onafhankelijk oordeel wordt gevormd over één of meerdere aspecten van een te onderzoeken object. Cruciaal is om goed vast te stellen welke objecten men gaat onderzoeken en op welke aspecten het onderzoek zich concentreert.

Fase vier is de *oplevering* van de resultaten, waarbij de terugkoppeling van de auditresultaten plaatsvindt. Aandachtspunt hierbij is de keuze om de rapportage in beperkte kring plaats te laten vinden of de resultaten ook openbaar te maken. Dit heeft ook consequenties voor de wijze waarop de verslaglegging plaatsvindt, bijvoorbeeld in rapport- of presentatievorm.

Ten slotte speelt het opvolgen van bevindingen, conclusies en aanbevelingen een rol: het is goed om vooraf stil te staan bij de consequenties die verschillende uitkomsten van het onderzoek zullen of kunnen hebben. In dit kader kan een opdracht in eerste instantie bewust oriënterend van aard zijn waarna men, afhankelijk van de uitkomsten, een diepgaander onderzoek start.

Kiezen van een passende auditvorm

Een belangrijk punt bij het formuleren van de opdracht is het kiezen van een passende auditvorm. Er bestaan meerdere soorten trajecten waarin een oordeel over iets wordt gegeven. Als er behoefte is aan een formele vaststelling, zoals bijvoorbeeld in het geval van een conflict of een financiële kwestie, dan ligt een formele audit voor de hand. Is er echter sprake van een meer oriënterende situatie dan komen *second opinions* of *quickscans* in beeld. Een zeer formele audit is dan een te zwaar middel. Hierna volgt een overzicht van een viertal vormen van beoordeling van een bepaalde situatie, namelijk de formele

audit, het vraaggestuurd onderzoek, de *second opinion* en de *quickscan*. Deze opsomming is niet limitatief; het is zeer goed mogelijk om bijvoorbeeld verschillende aspecten van de genoemde trajecten te combineren al naar gelang de specifieke omstandigheden.

Formele audit: bij het uitvoeren van een formele audit hanteert men veelal een bestaand normenkader, waartegen een toetsing van het te onderzoeken object plaatsvindt. Door zich te beperken tot de voorgeschreven normen zullen de uitkomsten van de audit zich beperken tot het objectief vaststellen of aan de normen wordt voldaan of niet. De eigen visie van de auditor of interpretatie van

Een audit is ook goed bruikbaar om de huidige stand van zaken weer te geven

waarnemingen wordt in dit soort trajecten buiten beschouwing gelaten. Voorbeelden van veelgebruikte normenkaders in de ICT zijn de code voor informatiebeveiliging, Prince2 (voor de inrichting en uitvoering van projecten), Cobit (voor het inrichting van IT-governance), ITIL (voor de inrichting en uitvoering van ICT-beheer), contractvoorwaarden en programma's van eisen.

Vraaggestuurd onderzoek: bij deze variant geeft de opdrachtgever vooraf aan op welke vragen hij of zij een antwoord zou willen hebben. De vragen bepalen de richting van het onderzoek, en het wordt dus niet gestuurd door een te hanteren normenkader. De onderzoeker heeft hierdoor meer vrijheid om te bepalen op welke wijze

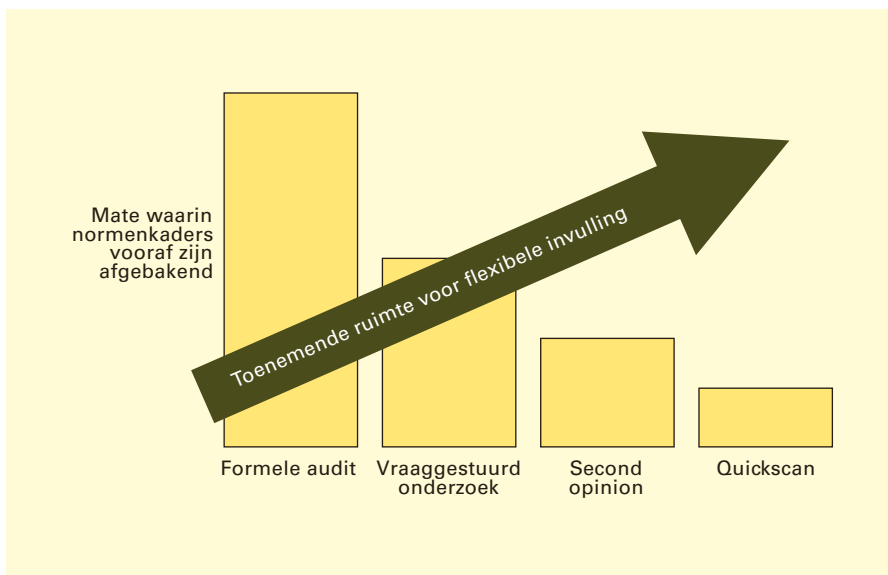
Losse pols

Het uit de losse pols verstrekken van opdrachten voor het uitvoeren van audits leidt in de praktijk tot verschillen van inzicht tussen de opdrachtgever en uitvoerder. De opdrachtgever moet zijn opdracht zorgvuldig formuleren, waarbij hij zelf duidelijk voor ogen heeft welke resultaten nodig zijn. Dit voorkomt dat pas aan het einde van de opdracht verschillen in perceptie met betrekking tot opdracht, vorm en proces naar voren komen, waarmee ook de bevindingen van een audit in het geding komen. Dit sluit aan bij de visie van professor De Caluwé in *Business Process Magazine* 5 van september 2004, waarin hij aangeeft dat "de formulering van de adviesvraag sterk bepalend is voor de kwaliteit van het advieswerk".

hij te werk gaat en er is hierdoor in het algemeen ook meer ruimte voor eigen meningen of interpretaties.

Second opinion: deze vorm van beoordelen, die we ook wel expert opinion of contra-expertise noemen, laat de auditor nog meer vrijheid in de wijze waarop de uitvoering van de opdracht plaatsvindt. Het is mogelijk om een *second opinion* uit te voeren aan de hand van een vooraf vastgesteld normenkader, maar de expert kan ook geheel vanuit zijn eigen deskundigheid een oordeel over het te onderzoeken object geven. Het verdient wel aanbeveling om vooraf met de opdrachtgever expliciet te maken in welke mate subjectiviteit een rol mag en zal spelen.

Quickscan: de *quickscan* leent zich, zoals de naam al aangeeft, uitstekend voor het verkrijgen van een snel en globaal oordeel over een onderzoeks-



Afbeelding 2. Vergelijking tussen auditvarianten.

object. Met de resultaten van de quickscan kan men vaststellen in welke richtingen verder onderzoek of ontwikkeling zou moeten plaatsvinden. De quickscan kan de basis leggen voor het formuleren van een aantal onderzoeksvragen zoals bij 'vraaggestuurd onderzoek' beschreven.

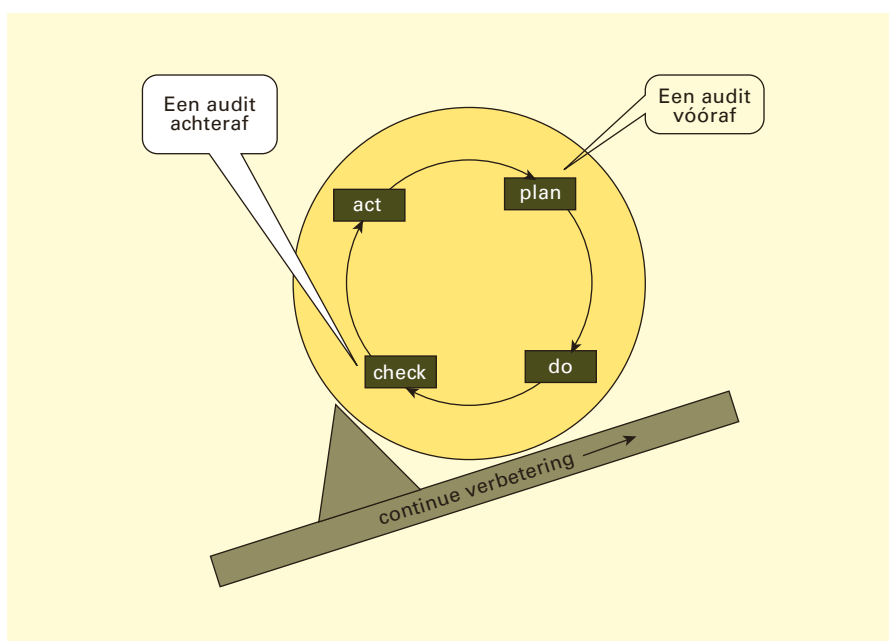
Centraal in de beschreven auditvarianten staat het feit dat er een *oordeel* over iets wordt gegeven; dit is als het ware het gemeenschappelijke kenmerk. Bij het uitvoeren van een formele audit dient een normenkader beschikbaar te zijn of te worden opgesteld. Het uitvoeren van een toetsing ten opzichte van dit normenkader geeft een objectief oordeel over de situatie. Niet in elke situatie zal een van tevoren geformaliseerd normenkader aanwezig zijn of is een zekere mate van subjectiviteit in het te hanteren kader gewenst. In deze gevallen zijn de andere verschijningsvormen vaak bruikbaar. Het een en ander is gevisualiseerd in afbeelding 2: naarmate de kaders van het onderzoek meer zijn afgebakend is er minder ruimte voor vrije interpretatie. Voor sommige trajecten zal dit zeer gewenst zijn, voor andere werkt dit beperkend. Dit benadrukt nogmaals

het belang van het kiezen van een passend traject. Het volgende voorbeeld geeft inzicht in het proces voor het maken van een bewuste keuze tussen de verschillende verschijningsvormen van audits.

Een directeur van een middelgroot bedrijf is benieuwd of het uitbesteden van een aantal ICT-activiteiten aan een derde partij interessant voor zijn bedrijf zou kunnen zijn. Hij reali-

seert zich dat het van belang is om eerst een goed beeld te krijgen van de huidige stand van zaken binnen het bedrijf, alvorens concrete stappen te ondernemen. Zo'n analyse, waarin diverse aspecten van de ICT-organisatie worden belicht, geeft een basis voor een passende uitbestedingsstrategie maar kan ook aanleiding zijn om eerst nog aanvullende maatregelen te treffen alvorens over te gaan tot uitbesteding. Tegelijkertijd realiseert de directeur zich dat hij als opdrachtgever voor zichzelf eerst een aantal vragen zal moeten beantwoorden om zoveel mogelijk voordeel uit de opdracht te halen.

De analyse uit voorgaand voorbeeld is in te vullen door middel van een audit die voorafgaand aan eventuele te ondernemen stappen op het gebied van outsourcing plaatsvindt. Het is in wezen een onderzoek of aan basisvoorwaarden voor een succesvol outsourcingtraject wordt voldaan. Deze basisvoorwaarden vormen eigenlijk het normenkader voor het onderzoek. Omdat de basisvoorwaarden geen wet van Meden en Perzen vormen maar voor elke organisatie



Afbeelding 3. Auditmomenten binnen de Deming-cirkel.

en situatie verschillend kunnen zijn, ligt de variant *formele audit* niet voor de hand. In deze situatie past wellicht de expert opinion-variant beter, of een compacte quickscan om een snelle analyse van de situatie te maken. Dit kan bijvoorbeeld leiden tot het opstellen van een normenkader, waaraan door middel van een uitgebreidere variant een toetsing kan plaatsvinden.

Tijd voor een audit

Het is gebruikelijk om een audit in te zetten ter controle achteraf. Hiermee kan een organisatie nagaan of gestelde doelen zijn behaald en of de resultaten aan bepaalde criteria voldoen. In de meest voorkomende variant is de audit gericht op het verleden. Het doel is om een oordeel te krijgen over iets dat inmiddels is afgerond.

Een audit is echter ook uitstekend bruikbaar om, voorafgaand aan nieuwe ontwikkelingen, de huidige stand van zaken in kaart te brengen. Door op de hoogte te zijn van de huidige situatie kunnen betere plannen worden gemaakt. Deze hebben over het algemeen een hogere kans van slagen dan plannen waarin een beeld over de huidige situatie ontbreekt. De audit fungeert in dit geval als nulmeting.

Beide momenten voor het uitvoeren van audits zijn weergegeven in de Deming-cirkel in afbeelding 3. Het doorlopen van deze Deming-cyclus en het inbouwen van toetsmomenten in zowel de *plan*-als in de *act*-fase zal leiden tot de beoogde continue verbetering.

Grip

In dit artikel is een aantal handreikingen gegeven die opdrachtgevers in staat stellen meer grip te krijgen op de uitvoering van audits. Het succes van een audit wordt vergroot wanneer de opdrachtgever een duidelijke visie heeft op de auditvorm, de verschillende auditfasen en het gebruik

Meer ICT-audits?

In de nabije toekomst zal de hoeveelheid ICT-audits dat wordt uitgevoerd waarschijnlijk toenemen. Hier ligt een aantal ontwikkelingen aan ten grondslag. Ten eerste neemt de informatieafhankelijkheid van organisaties sterk toe. Wanneer ICT-voorzieningen niet beschikbaar zijn dan heeft dit directe consequenties voor de uitvoering van de bedrijfsprocessen. Een duidelijk beeld van de status en de kwaliteit van interne en externe dienstverlening en toegepaste middelen is essentieel om sturing te kunnen geven. Door verregaande integratie tussen infrastructuur, hardware, standaardpakketten en applicaties neemt de complexiteit toe. Toenemende afhankelijkheid én toenemende complexiteit zijn elkaar versterkende factoren als het gaat om de kwetsbaarheid van reeds geautomatiseerde bedrijfsprocessen, maar zeker ook voor toekomstige plannen op dit gebied. Audits kunnen in deze gevallen duidelijkheid geven en een kader vormen voor verdere ontwikkeling.

Een tweede reden is dat organisaties het zicht op de ICT kwijtraken. Bij veel organisaties heeft het fenomeen outsourcing zijn intrede heeft

gedaan of zal dit binnenkort wellicht gaan doen. Hierdoor wordt de afhankelijkheid van externe diensten- en productenleveranciers groter. De opdrachtgeversorganisatie concentreert zich meer en meer op het primaire proces en diepgaande ICT-kennis wordt schaarser binnen de eigen organisatie. Doordat ICT-activiteiten veelal op afstand worden uitgevoerd is het lastiger om een goed beeld te krijgen van de wijze waarop de dienstverlening is ingericht en hoe resultaten tot stand komen. Ook het extern laten ontwikkelen van bedrijfsapplicaties en het toenemende gebruik van standaardsoftware kunnen oorzaken zijn van verminderd inzicht in de ICT. Door middel van het uitvoeren van een audit is op gestructureerde wijze de ICT-dienstverlening inzichtelijk te maken.

Ten slotte is er wetgeving, zoals Sarbanes-Oxley, die de nodige claims op het adequaat functioneren van ondermeer ICT-systemen legt. Ook in deze gevallen kan via audits worden aangetoond dat aan de gestelde eisen is voldaan of aangegeven waar verbeteringen nodig zijn.

van de auditresultaten. Door zelf voldoende tijd en energie te steken in de voorbereiding houdt de opdrachtgever grip op het proces en zullen de uitkomsten van de audit een waardevolle informatiebron zijn voor verdere optimalisatie van de bedrijfsvoering door middel van ICT. Uiteindelijk komt het natuurlijk neer op een samenspel tussen opdrachtgever en uitvoerder, waarbij verwachttingsmanagement over en weer een centrale plaats inneemt.

Literatuur

1. J. van Praat en H. Suerink, Inleiding EDP auditing, Ten Hagen Stam, 1992.
2. Ir. P.J. Scheffel e.a., Het doel, de weg en de rugzak, een gids voor praktisch ICT service management, Van Haren Publishing, 2004.
3. W.E. Deming, Quality, Productivity and Competitive Position, MIT Center for Advanced Engineering Study, Cambridge, 1982.

Chris Neuteboom en Bram Spitzer

Chris Neuteboom is adviseur bij Verdonck, Klooster & Associates (chris.neuteboom@vka.nl).
Bram Spitzer is tevens adviseur bij Verdonck, Klooster & Associates (bram.spitzer@vka.nl).