

een systeemverantwoordelijkheid. BZK heeft een bureau ingericht voor de uitvoering van zogenaamde Gateway-reviews. Verder is afgesproken dat BZK jaarlijks één rapportage voor de Tweede Kamer(TK) over alle grote ICT-projecten (en projecten met een grote ICT-component) binnen de rijksoverheid verzorgt.

Eelke gaat in op de vraag wanneer in de praktijk de auditor bij ICT-projecten in beeld komt? Haar ervaring is dat dit per departement verschilt. Sommige auditors rapporteren vooral vanuit de wettelijke taak. Bij andere departementen wordt meer vanuit een vraaggestuurde opdracht gerapporteerd. Het criterium van € 20 mln is lang niet altijd bepalend voor het uitvoeren van een audit. De opdracht wordt vaak verstrekt vanuit een bepaalde risicoperceptie. De auditfunctie rond grote ICT-projecten is nog in ontwikkeling, daar is ook een IODAD-brede werkgroep voor opgericht. De AD's van departementen waar veel grote ICT-projecten plaatsvinden zijn actiever betrokken tijdens het project met vaak een bredere focus dan het financieel beheer. Verder zijn er nog veel verschillen in terminologie en benoemen auditors in hun aanpak elementen/aspecten verschillend. Ook verschillen rapportages ten aanzien van effecten en conclusies. "Dit maakt het ook lastig om van elkaar te leren" vult Chris aan. Juist op dat punt kan Gateway als 'peer-review methode' een belangrijke rol spelen. Een belangrijke nevendienststelling, naast meer succesvolle projecten uitvoeren, is het van elkaar leren.

Het is de rol van BZK om over de bevindingen aan de TK te rapporteren, aldus Roel. Soms zijn er ook meerdere opdrachtgevers (departementen) betrokken. Om efficiënter te werken en meer eenduidigheid te krijgen is in het IODAD besloten om vanaf 2010 gezamenlijk op trekken bij het plannen van audits op het gebied van de rijksbrede bedrijfsvoering.

Welke competenties dient de onderzoeker of het onderzoeksteam voor een Gateway-review te bevatten?

Chris heeft zelf meerdere reviews gedaan en georganiseerd en spreekt uit ervaring dat een auditor in een reviewteam van toegevoegde waarde kan zijn. Auditors zijn namelijk gewend om in korte tijd een beeld te krijgen van de situatie. Ook hebben ze veel ervaring met op hoofdlijnen rapporteren en weten ze hoe ze de juiste, open vragen moeten stellen. 'Peers' in een reviewteam hebben daar over het algemeen wat minder ervaring mee. Wel vergt het meedoen in een Gateway-review wat van de flexibiliteit en van het adviserend vermogen van de auditor.

Wat is nu de meerwaarde van het verplicht laten reviewen van projecten?

Roel geeft aan dat de primaire doelstelling is het project verder te helpen. Dat gebeurt door op verschillende momenten, bij faseovergangen, te meten of de doelstellingen zijn gehaald en de risico's voldoende worden beheerst en door hierover op gestructureerde (standaard) wijze te rapporteren. Dat meten kan bijvoorbeeld gedaan worden met behulp van audits en Gateway-reviews. De opdrachtgevers/departementen bepalen zelf welk instrument ze

wensen in te zetten. Chris heeft samen met een collega-auditor van het Ministerie van Economische Zaken de verschillen tussen audits en Gateway-reviews al eens uiteengezet in een artikel in de EDP-auditor in 2007. Reviews worden uitgevoerd door collega-ambtenaren die op hetzelfde terrein werkzaam zijn. Audits worden uitgevoerd door opgeleide auditors die gehouden zijn aan strikte beroepsregels. Daarnaast zijn auditrapporten vaak meer verantwoordend; reviewrapporten zijn meer adviserend van aard. Bij Gateway-reviews is ook geen sprake van harde vastgestelde normen. Wel zijn er handboeken op basis waarvan de aandachtspunten en vragen worden opgesteld. Ook verschillen aanpak en werkwijze en de verspreidingskring van de rapportage. Een Gateway-review duurt maximaal één week van begin tot eind, inclusief de rapportage. Een belangrijk verschil met een audit is ook dat aan het eind van een Gateway-review alle informatie vernietigd wordt die het reviewteam heeft vergaard. Alleen de rapportage blijft over. Een 'audittrail' is dan ook niet voorhanden.

De door DGOBR in de kaders benoemde faseovergangen zijn volgens Eelke in praktijk niet altijd even duidelijk bij projecten en programma's terug te vinden. Door auditors wordt vaker gekozen voor periodieke rapportage in plaats van na afronding van een bepaalde fase. Chris herkent dit en geeft aan dat het bij Gateway-reviews van overheidsprojecten ook niet altijd eenvoudig is om met de opdrachtgever vast te stellen welke review van toepassing is. Bij Gateway hanteert men kleuren voor de aanbevelingen van rood tot groen waarbij "rood" staat voor "direct actie ondernemen" alvorens naar de volgende fase over te gaan. Uiteindelijk beslist de opdrachtgever of verder gegaan wordt met de volgende fase en niet de reviewer(s).

De TK zal vanaf voorjaar 2009 jaarlijks een rapportage inclusief overzicht met lopende ICT-projecten ontvangen waarin zij over de uitvoering en de resultaten hiervan wordt geïnformeerd. Volgens Roel wordt in de rapportage in ieder geval ingegaan op de geraamde versus de werkelijke kosten en de geraamde versus de werkelijke doorlooptijd. Daarnaast wordt gerapporteerd over de mate waarin ministeries zich houden aan de afspraken over projectplannen en reviews.

Tot slot de vraag wat de volgende stap is in het proces van beheersing van ICT-projecten?

Wat kunnen we verbeteren? Unaniem is men van mening: "het control framework completer maken!" Met het uiteindelijke doel dat de uitvoering van projecten en programma ook daadwerkelijk verbeteren. Instrumenten als audits en Gateway-reviews moeten in hun onderlinge samenhang gezien worden. Met de kanttekening dat daar harmoniseren van de rapportages, de bevindingen vergelijken en leren van elkaars goede punten en fouten, problemen en oplossingen bij horen. Daarnaast zou er ook meer aandacht moeten komen voor het niveau boven de individuele projecten. Op dat niveau moet geborgd zijn dat de juiste projecten worden gestart en dat de afhankelijkheden en samenhang tussen projecten bewaakt worden. «



**'Een schot in het donker'**  
Chris Verhoef over de uitdagingen bij het auditen van grote IT-projecten en verschillen tussen de overheid en het bedrijfsleven.

DOOR ROOS KALKER EN SANDER VAN DER KRAAN

Wat zijn factoren voor het slagen en falen van IT-projecten? En zijn er hierbij verschillen tussen de rijks-overheid en het bedrijfsleven waar te nemen? Welke rol kan een auditor spelen? En wat zijn de laatste ontwikkelingen in de wetenschap?

ZIEN(\*) sprak hierover met Chris Verhoef, hoogleraar Informatica aan de Vrije Universiteit van Amsterdam.

### 1. Overheid versus het bedrijfsleven

“De risico’s bij grote IT-projecten bij de overheid zijn in de meest conservatieve modellen al twee keer zo hoog vergeleken met het bedrijfsleven!”, vertelt Chris Verhoef. Dit bleek uit een onderzoek bij de overheid en 6000 projecten in de private sector. Volgens Chris zijn er verschillende oorzaken voor dit fenomeen.

#### Voor de volle 100 procent

De ambitie bij het Rijk ligt bij IT-projecten altijd veel hoger dan bij het bedrijfsleven, soms op het onrealistische af. Het Rijk wil vaak heel de IT-oplossing in één keer realiseren: zowel intern (back-office) als richting de burger (front-office). Het bedrijfsleven is daar

veel realistischer in. Zij willen ook een optimaal eindproduct, maar beginnen vaak met eerst eens tachtig procent. De laatste twintig procent kost naar verhouding veel inspanning en doet het bedrijfsleven niet als dit niet nodig is.

Chris: “Het vraagt een omslag in het denken bij het Rijk om niet direct voor de volle honderd procent te willen gaan. Een voorbeeld van een project waarbij in eerste instantie direct voor de volle honderd procent is gegaan P-Direkt. Een personeelsadministratie voor het Rijk in een keer implementeren is natuurlijk een enorm risico.”

#### Eerst de bedrijfsprocessen, dan de IT

Een ander verschil tussen het bedrijfsleven en de overheid is dat de overheid vaak niet denkt in netto contante waarde. Wat moet een IT-project eigenlijk opleveren? En is een nieuw IT-systeem wel de oplossing voor het probleem? Chris verduidelijkt: “In de Verenigde Staten moet je - als je als overheidsorganisatie een nieuw IT-systeem wil laten ontwikkelen - eerst het bedrijfsproces in kaart brengen. Wanneer dat eerste geoptimaliseerd is, implementeer je in ieder geval geen obsoleet bedrijfsproces in de IT.” Bij de Rijksoverheid worden echter vaak incidentgedreven oplossingen gekozen, als iets politiek actueel is. “Bijvoorbeeld het elektronisch patiëntendossier. Het idee achter dit project is dat wanneer alle patiënten in het systeem zitten, je geen contra-indicaties of medische missers meer zou hebben. Dit is echter vooral van groot belang voor 3% chronisch zieken die ons land kent. En bovendien zou je deze informatie uit de administraties van de verzekeringsmaatschappijen kunnen krijgen.” licht Chris toe.

#### IT-kennis en de Balkenende norm

Volgens Verhoef kijkt de overheid ook niet goed of er voldoende kennis in huis is om een project tot een succesvol einde te brengen en of er niet beter iemand kan worden ingehuurd met kennis van zaken die de regie gaat voeren. Chris: “De overheid zou zich moeten afvragen of zij wel aantrekkelijk genoeg zijn voor top IT-ers. Is de overheid bereid de Balkenende norm te laten varen om top IT-ers een marktconform salaris te bieden?”

### 2. Beheersing van IT-projecten en de rol van audit

Om te bepalen of een IT project beheerst verloopt kun je kijken naar uitvoeringsrisico’s zoals budget, tijdsoverschrijding en de verkeer opgeleverde functionaliteit. Daarnaast kun je kijken of er een proces is geregeld. Chris: “Als je wilt oordelen hoe dit proces verloopt, is er echter niet één checklist om dit in kaart te brengen. Het volgen van bijvoorbeeld de Prince2 methode is nog geen garantie voor succes. Maar je kunt wel degelijk oordelen hoe het met een project staat. Dat vergt alleen veel meer creativiteit en diepgravend onderzoek naar alle artefacten die er van een project zijn.”

#### Een schot in het donker

Bij de start van een audit is het wel van belang om zoveel mogelijk gegevens op te vragen. Helaas blijkt in de praktijk dat de adminis-

tratie van IT-projecten niet altijd even volwassen is geregeld. “De Algemene Rekenkamer heeft geprobeerd IT-projecten aan de hand van projectadministraties te onderzoeken. Maar projectadministraties leveren lang niet genoeg informatie om een diepgravend onderzoek te doen naar de status van een IT-project. Daarnaast heeft een slecht project ook een slechte administratie.” zegt Chris. Is het nu een taak van de IT-auditor om de beheersing van het IT-project te controleren? De vraag die je volgens Verhoef hierbij moet stellen is of de IT-auditor wel alle kennis in huis heeft die nodig is om tot een goed oordeel te komen. “Het is alsof je in het pikkedonker een schot hagel afvuurt om een haas te schieten.” vertelt Chris “Omdat er zoveel manieren zijn waarop mensen een IT-project inrichten en uitvoeren, is er niet één auditaanpak. Bij financiële audits is die er wel. Bij IT-projecten weet je niet precies wat je zoekt en bovendien kun je als toetsers van alles aantreffen”. Verhoef geeft aan dat het veel beter is om bij een onderzoek naar de projectbeheersing een multidisciplinair team in te zetten dat verschillende expertises op gebied van IT en de beheersing van IT-projecten bezit en daardoor vanuit verschillende kanten kan onderzoeken.

#### Auditor bij de start van een IT-project

De toegevoegde waarde van de auditor zit volgens Verhoef ook bij de start van een IT-project. Want hoe vroeger je toetst, hoe meer je kunt bijsturen. Voordat een project van start gaat, zou allereerst een ICT-haalbaarheidstoets moeten plaatsvinden. Dit wordt bij het Rijk momenteel aan het bedrijfsleven gevraagd, maar je zou zo’n haalbaarheidstoets als overheid juist zelf moeten uitvoeren om belangenverstrengeling te voorkomen. Daarnaast blijkt de (rijks)overheid bij aanbestedingen vaak voor het bedrijf dat de laagste prijs biedt te kiezen. Chris: “Dit komt omdat de kwaliteit onvoldoende verdisconteerd wordt in de gebruikte prijs-kwaliteitsmodellen.” Volgens Chris zou de overheid zich hierbij de vraag moeten stellen of dan ook de beste kwaliteit wordt geleverd. De toetsers van een aanbesteding zouden in hun beoordelingscriteria voor offertes meer kwaliteitcriteria moeten opnemen. “Zowel bij de haalbaarheid als bij de aanbesteding kunnen de auditors een rol spelen.” zegt Chris.

#### De CIO als machtige man

Verhoef vind de komst van een Chief Information Officer voor het Rijk in Nederland een goede zaak. Hij zou de Rijks CIO willen adviseren om vaste toetsmomenten door middel van het uitvoeren van audits of peer-reviews op te nemen in de manier waarop de Rijksoverheid projecten aanpakt. Voor het succes van de Rijks CIO is het belangrijk dat hij ook de bevoegdheid krijgt om een project niet door te laten gaan op het moment dat het niet door de beugel kan. Chris: “Wanneer gekeken wordt naar de aanbesteding van IT-projecten door de overheid in de Verenigde Staten, dan zie je dat daar de CIO de macht heeft om een Go-No go beslissing te nemen. In de VS wordt ook gewerkt met de zogenoemde ‘Raine’s Rules’. Dit zijn 8 punten waaraan een projectvoorstel minimaal moet voldoen. Als dat niet klopt kun je sowieso niet door. Als er wel aan voldaan is, heb je de eerste horde genomen maar toestemming heb je nog niet. Voorbeelden van deze Rules zijn dat je niet iets gaat laten ont-

wikkelen wat een andere overheidsinstantie al in gebruik heeft en je zo kunt gaan gebruiken, dat je niet iets gaat ontwikkelen wat kant-en-klaar te koop is en dat je het risico bij acquisitie moet spreiden tussen jou als opdrachtgever en de leverancier. Deze regels zijn mogelijk ook toepasbaar in Nederland.” Vooralsnog blijkt in Nederland dat de urgentie niet zo hoog is om dit alles naar Amerikaans voorbeeld door te voeren.

#### Transparantie van een onderzeeër

Transparantie bij een IT-project is heel belangrijk. Dat transparantie kan leiden tot significante verbeteringen is bekend in de wereld van de onderzeeërs. Chris: “Daar heeft de commandant een logboek op tafel liggen waarin iedereen elke dag zijn fouten optekent. Iedereen maakt fouten, dus elke dag meld je die. Sta je er een dag niet in, dan is dat op zich al een fout. De fouten worden onderling besproken om er zo voor te zorgen dat door honderd procent transparantie alles in het werk wordt gesteld om samen te voorkomen dat de onderzeeër zinkt. Ook bij IT-projecten moet die openheid over wat er goed of fout gaat er zijn. Dat kan door het goed bijhouden van een projectadministratie in combinatie met het op vaste momenten gedurende het proces een review uit te voeren.”

### 3. Ontwikkelingen in de wetenschap

ZIEN(\*) vraagt Chris Verhoef naar welk aspect van grote IT-projecten hij momenteel zelf onderzoek doet. Hij geeft aan dat hij vanuit de Vrije Universiteit samen met een groep van onderzoekers van verschillende IT-disciplines kijkt naar grote IT-complexen bij grote Nederlandse industriële bedrijven. Er wordt in het onderzoek bijvoorbeeld gekeken naar embedded-systemen, zoals optica, medische apparatuur en defenisiesystemen. Een van de onderwerpen van onderzoek is daarbij hoe de software in die systemen of losse hardware is geprogrammeerd. Dit soort IT-onderzoek staat echter nog in de kinderschoenen.

#### Wat zit er in de doos?

De uitvoeringsorganisaties van de overheid behoren tot de top 25 groot verbruikers van IT in Nederland. De belangrijkste enabler – de IT – van deze organisaties staat vaak niet onder een auditregime. Chris: “Bij IT is het van belang om niet alleen te kijken naar de beheersing van het proces, maar je moet je ook altijd afvragen wat er in de doos zit, in het systeem duiken. Vragen die je daarbij kunt stellen zijn de continuïteit van de dienstverlening, de onderhoudbaarheid en de efficiëntie. Is het systeem wel veilig? En was het dit gisteren, is het dat vandaag en zal het dat ook morgen nog zijn?” De inrichting van een IT-systeem zou je dan ook empirisch moeten onderzoeken.

IT-systemen en projecten zijn complex en kennen veel verschillende dimensies. Deze complexiteit betekent echter niet dat je geen onderzoek kan doen. Het vergt alleen creativiteit en diepgravend onderzoek naar alle artefacten die er van een project of IT-systeem zijn. Het duiken in het IT-systeem hoort hierbij. «