Scenariodenken

De zekerheid van onzekerheid

Ronald Robbers

We leven nu eenmaal in een maatschappij waarin bijna alles met alles te maken heeft en waarbinnen in toenemende mate 'dat alles' elkaar wederzijds beïnvloedt. Zekerheid moet als een schaars goed worden beschouwd. Immers, veel wederzijdse afhankelijkheden en beïnvloedingen zijn niet of nauwelijks direct te beïnvloeden.
Hoe gaat de auditor te werk in werelden van grote complexiteit en dus per definitie relatief grote onzekerheid; blijven we zoeken naar gewenste zekerheid (complexiteitsbeheersing) of is het wellicht handiger om ons te richten op eliminatie van onzekerheid (complexiteitsreductie)?

Inleiding

Begrippen als 'complexiteitstoename' en 'sneeuwbaleffect' zijn aan de orde van de dag. De IT draagt daaraan bij als enabler voor bedrijfsoverstijgende integrale procesondersteuning door te zorgen voor een extra vervlechting van vele procesinrichtingen en -beheersingen. Daarnaast zijn de te beantwoorden auditvragen steeds breder en betreffen soms hele organisaties in één keer in plaats van een autonoom deelobject. De complexiteitstoename is vanuit beide invalshoeken – procesvervlechtingen en bredere vraagstellingen – goed merkbaar; de auditor krijgt steeds meer werk met het vaststellen of de gebruikte SOLL wel de gewenste zekerheid op kan leveren. Immers, hoe weet de auditor zeker of de voorgestelde set maatregelen nu en in de toekomst met al die wederzijdse afhankelijkheden wel toereikend is?

Door verschillende scenario's naast elkaar te leggen kan het potentiële resultaat van een set maatregelen — uitgedrukt in zekerheden en financiële impact — worden geanalyseerd. Daarbij kan zekerheid worden gezien als een soort resource die als het ware ingepland moet worden. En volgens mij is onzekerheid dat in zekere zin ook. Deze bijdrage betreft een voorzet voor het scenariodenken als auditinstrument en doet dat vanuit de gedachte dat zowel het verkrijgen van zekerheid als het elimineren van onzekerheid daarbij als input kan dienen.

Ir. R.M.R.Robbers RE CISA CIA is werkzaam als accountmanager/clustercoördinator 'materieelprocessen' bij de IAD van de Nederlandse Spoorwegen. Dit artikel is op persoonlijke titel geschreven.

Scenariodenken

Zekerheden en onzekerheden kunnen in scenario's worden uitgezet om een toekomstbeeld te bepalen. De gewenste beheersing van het auditobject kan aan één of meerdere toekomstbeelden worden gerelateerd. Het betreft hier een analysemodel voor auditors en managers bij prospectieve vraagstukken naar de toereikendheid van beheersingsaspecten.

Door de huidige en alternatieve vormen van de beheersing van het auditobject te relateren aan mogelijke toekomstbeelden ontstaat een analysemodel waarvan de uitkomsten kunnen worden gebruikt voor verbetervoorstellen in die beheersing. Om dat goed duidelijk te maken, eerst een toelichting bij het begrip complexiteit.

Complexiteit

IT-objecten ontlenen hun betekenis vaak verregaand aan de organisatorische – en daarmee aan een continu veranderende – context en hebben veel veranderlijke relaties tussen de vele verschillende objectelementen. Ontwikkelingen in en rond organisaties worden steeds meer getypeerd als van toenemende dynamiek en com-

plexiteit [PIJL00]. Hierover is vanuit diverse invalshoeken al veel geschreven. Drie voorbeelden:

Al in 1992 wordt door het NGI [NGI92] onderkend dat binnen de risicoanalyse de diverse verbanden tussen de te onderzoeken objecten moeten worden meegenomen.

Vanuit de invalshoek 'complexiteitsbeheer' hebben Jan Truijens en Joop Winterink reeds in 1996 een artikel in *de EDP-Auditor* geschreven met de titel 'Complexiteitstoename van de (geautomatiseerde) informatieverzorging' [TRUIJ96]. Hierin wordt onder meer door het actualiseren van de traditionele onderzoeksobjecten voor de IT-auditor enerzijds en het structureren van de relaties daartussen anderzijds een aangepast beheerskader gegeven. Zij verwachtten destijds al een vernieuwende taakopvatting en -uitoefening van de IT-auditor op onder meer het gebied van complexiteit.

Met een andere invalshoek, nl. via de 'risicobeheersing', heeft Ted Mos in 1998 een artikel geschreven, eveneens in *de EDP-Auditor*, met de titel 'Het (accountants?) auditrisk voor IT-auditing beschouwd' [MOS98]. De traditionele risicoformule voor IT-auditors wordt hier onder de loep genomen en er wordt een voorstel gedaan voor een herziene versie welke zich meer richt op beïnvloedbare items van de IT-audit dan tot dan toe gebruikelijk. Mos hanteert een meerdimensionaal model voor het IT-auditrisk. Immers – zo stelt Mos – het mag duidelijk zijn dat het beheersbaar maken van de risico's die de IT-auditor loopt tijdens zijn werkzaamheden, een samenspel is van veel componenten, met een eigen uitwerking en bereik.

Wanneer is iets complex? De termen complex of simpel geven geregeld aanleiding tot discussie [EDP01].
Er bestaan vele definities welke voor een bepaalde invalshoek de mate van complexiteit aan een object koppelen door deze uit te drukken in een numerieke waarde. Dergelijke metrieken geven echter niet aan wát de complexiteit is, waar die zich bevindt of wat de oorzaak ervan is. Verder zijn dergelijke definities veelal beperkt tot een zeer specifieke verzameling van (typen van) onderzoeksobjecten terwijl de auditor met een breed scala aan onderzoeksobjecten te maken heeft.

Wat is dan wel complexiteit? Zie het auditobject als een het dynamische geheel van min of meer autonome deelobjecten die voor de audit separaat beschouwd moeten worden, onderling relaties kunnen hebben, elkaar kunnen beïnvloeden, wel of niet beïnvloedbaar zijn met beheersmaatregelen, en waarbij de objecten en relaties veranderlijk kunnen zijn in zowel aantal als soort.

Je zou het auditobject dan kunnen visualiseren door verschillende bolletjes (deelobjecten) met diverse soorten pijltjes ertussen (relaties). Een grafische weergave van het in kaart brengen van risico's en gevolgen die aansluit bij de hier gebruikte definitie van complexiteit waarbij objecten door relaties aan elkaar verbonden zijn is beschreven door Herrera in zijn artikel Graphical Risc Analysis [HERR02].

Vanuit deze gedachte kan complexiteit worden gezien als het verschil tussen het totale dynamische geheel van die deelobjecten en relaties enerzijds en het statische totaal van de losse deelobjecten anderzijds. Complexiteit is daarmee afhankelijk van de auditscope *(die voor de audit separaat moeten worden beschouwd)*, is tijds- en contextafhankelijk *(dynamische geheel … veranderlijk in aantal en soort)* waarbij er rekening moet worden gehouden met onderdelen die wel van invloed zijn op de gewenste beheersing maar waarop we geen invloed kunnen uitoefenen *(wel of niet beïnvloedbaar zijn)*. Hierdoor heeft complexiteit meestal een bepaalde mate van onvoorspelbaarheid in zich.

Twee denkwerelden

Een dergelijk model van een dynamisch geheel aan deelobjecten en tussenliggende relaties ('bolletjes en pijltjes') kan op verschillende manieren worden bekeken. Ik wil hier twee van dergelijke denkwerelden onderscheiden.

De eerste denkwereld heet 'zekerheid is een resource' en beschrijft de situatie waarin het gehele auditobject tot in detail kan worden beschreven en geanalyseerd en daarmee geheel voorspelbaar wordt. De tweede denkwereld heet 'onzekerheid is een resource' waarin het auditobject als een verzameling autonome deelobjecten wordt gezien die relaties met elkaar aangaan. Beide denkwerelden worden hierna toegelicht.

Zekerheid is een resource

In de denkwereld 'zekerheid is een resource' wordt het auditobject gezien als een groot geheel dat tot in de kleinste details kan worden beschreven en geanalyseerd. Daarbinnen kan door een juiste (risico)analyse het gedrag van dat object als geheel inzichtelijk en voorspelbaar worden gemaakt. Door de beheersmaatregelen op die analyse aan te sluiten is de gewenste beheersing en zekerheid voorspelbaar. Dit is de risicoanalytische aanpak.
De beheersing wordt topdown in kaart gebracht omdat de aansturing centraal geschiedt. Ervaringen uit het verleden, toekomstverwachtingen en actuele feiten zijn de basis voor de beheersmaatregelen. De maatregelen zijn veelal gebaseerd op gewenste zekerheden en komen terug in de SOLL bij diverse audits.

In deze denkwereld moet voor elk risico een maatregel in werking treden die het object op een adequate wijze behoedt voor negatieve gevolgen. Ik noem dit een regelgeoriënteerde denkwereld; bij elk risico hoort een maatregel vaak in een als-dan afspraak vervat.

Zekerheden worden in deze denkwereld vanuit een centrale aansturing beheerst doordat control op een voldoende hoog niveau is ingericht en de verantwoording ervan centraal is belegd. Risico's van verstoring van het systeem kunnen aldus rationeel worden benaderd en gemitigeerd door (aanvullende) centrale sturingsmogelijkheden; een bijna mechanistisch wereldbeeld waarbij alles via denkbeeldige radertjes in vaste patronen op voorspelbare wijze werkt.

Waarom een tweede denkwereld? Ik ben van mening dat deze eerste denkwereld op zich niet meer past bij de huidige realiteit; deze bijdrage moet dat duidelijk maken. Dat is ook precies de reden waarom ik de tweede denkwereld heb geïntroduceerd. Een denkwereld waarbij onzekerheden een grotere rol spelen. Immers, uitgaande van het bijna mechanistisch wereldbeeld 'zekerheid is een resource' kunnen auditors simpelweg redeneren dat een inventarisatie van afhankelijkheden en kwetsbaarheden (A&K-analyse) dé basis is voor de te treffen beheersmaatregelen. En dat is precies de valkuil waar ik het in deze bijdrage over wil hebben! Hoe bepaalt de auditor de (toereikende werking van de juiste) beheersingsmaatregelen als we met z'n allen eigenlijk niet goed weten waarvan we afhankelijk zijn? Of, hoe gaat de A&K-analyse als de A niet bekend is?

De tweede denkwereld gebruik ik om te onderstrepen dat niet de suggestie moet worden gewekt (door auditors, management, of wie dan ook) dat het afdekken van gevonden risico's op zich voldoende zekerheid zal brengen over beheersing in complexe situaties. Er moet ook rekening worden gehouden met mogelijk nog onbekende risico's.

Onzekerheid is ook een resource

Complexiteit gaat meestal gepaard met een bepaalde mate van onvoorspelbaarheid omdat een deel van de aansturing ongrijpbaar is. Kevin Kelly heeft hierover een boek geschreven: Out of control [KELLY94]. Een passage die wat mij betreft het verband tussen beheersing en complexiteit goed beschrijft, is te vinden op p. 603 in het hoofdstuk 'The Nine Laws of God'. Ik citeer daaruit het volgende: 'When everything is connected to everything … everything happens at once. When everything happens at once … problems simply route around any central authority. Therefore, overall governance must arise from the most humble interdependent acts done locally in parallel, and not from a central command. … To get something from nothing, control must rest at the bottom within simplicity.'

Met de locatie van het begrip simplicity *(must rest at the bottom)* geeft Kelly aan dat complexiteit ontstaat doordat alles met alles verbonden is of kan zijn. Hij beschrijft dat het auditobject een verzameling autonome deelobjecten is die relaties met elkaar aangaan. Door zorg te dragen voor juiste relaties en afspraken tussen die objecten is het gedrag van het object als geheel ineens beter voorspelbaar geworden. Door de beheersmaatregelen op die relaties en afspraken aan te sluiten is de gewenste beheersing en de ongewenste onzekerheid voorspelbaar.

De risicoanalytische aanpak sluit – denk ik – nog onvoldoende aan bij deze gedachte. De beheersing is immers decentraal en kan niet meer alleen met een standaard top-down-methode in kaart worden gebracht omdat de aansturing niet centraal geschiedt. Het gehele auditobject is een soort flexibele structuur van wat ik eerder autonome deelobjecten noemde. Een belangrijke basis daartoe zijn de afspraken en relaties (vertrouwen) gericht op control in de toekomst. Die afspraken worden gemaakt aan de hand van ongewenste onzekerheden; zij zouden ook onderdeel moeten uitmaken van de SOLL binnen diverse audits. Dergelijke afspraken zijn wat mij betreft principe georiënteerd *('We spreken af dat … verantwoordelijk is voor het niet laten voorkomen dat …')* in tegenstelling tot de veelal regelgeoriënteerde afspraken uit de andere denkwereld *('Als … dan moet … de actie … uitvoeren.')*.

Deze denkwereld – die van de onzekerheid – gaat uit van het basisprincipe dat de auditor niet goed weet waarvan de beheersing van het auditobject direct afhankelijk is. Vergelijk het met de mogelijke antwoorden op de vraag wat te doen tegen terrorisme.

In deze denkwereld moet op elke ongewenste afwijking van de zekerheid de afspraken/relaties tussen de objecten onderling een voldoende (principiële) basis bieden tegen negatieve gevolgen. Regels alleen werken niet meer afdoende omdat deze niet inspelen op nog onbekende situaties. Algemenere principes voorkomen negatieve gevolgen van risico's. De Corporate Governance code's zijn net als deze denkwereld ook grotendeels principegeoriënteerd; ze zijn gebaseerd op door meerdere partijen gedragen opvattingen en uitgangspunten.
(De code Tabaksblat bevat twintig van dergelijke principes.)

Schijnbare onzekerheden die vanuit een centrale aansturing niet kunnen worden beheerst, zijn nu ineens meer grijpbaar geworden door control op een voldoende laag niveau in te richten en de verantwoording en mogelijk zelfs de monitoring ervan decentraal te beleggen.

Resources moet je managen

Zelf ben ik van mening dat we door de complexiteitstoename van auditobjecten ons steeds meer moeten beseffen dat we niet kunnen volstaan met het zoeken naar zekerheid, maar ook gebruik moeten maken van het proactief elimineren van onzekerheid. Dus, een combinatie van de twee geschetste denkwerelden. (Hoe dat er in de praktijk uit zou kunnen zien, moet blijken uit het voorbeeld verderop.) Ik heb in dit kader al eens geschreven dat complexiteitsanalyse een welkome aanvulling kan zijn op de klassieke risicoanalyse (zie [ROBB02]). Alvorens in te gaan op hoe dat zou kunnen, een verfijning zonder verdere toelichting van beide denkwerelden in tabel 1 (zie p. 8).

Van onzekerheid naar scenariodenken

Een risico is de impact van een onzekere gebeurtenis op de gewenste doelstellingen die de auditor met de audit wenst te onderzoeken. Risico's worden gemeten in termen van impact en de kans van optreden [GLEIM01] en voor een betere voorspelbaarheid in de tijd hoort daar wat mij betreft ook de verwachte doorlooptijd van optreden bij. Immers, het optreden van een risico is vaak niet een moment, maar het risico manifesteert zich een bepaalde tijd. Als gevolg daarvan is een gewenste zekerheid uit te drukken in termen van maximale negatieve consequentie van een gegeven set van risico's. Dat kan bijvoorbeeld aan de hand van afhankelijkheden en kwetsbaarheden vanuit de risicoanalyse.

De SOLL gericht op het adequaat beheersen van risico's bestaat uit te treffen maatregelen. Dergelijke maatregelen (controls) zijn een door iets of iemand ondernomen actie om gewenste doelstellingen te bereiken [GLEIM01]. Die acties hebben een bepaald effect op het object van onderzoek. Dat effect is gericht op het verkleinen van de negatieve consequenties vanuit de risico's.

Maar omdat de 'wederzijdse beïnvloeding' ook uit te drukken is in acties en kansen van optreden bestaat daarmee een uniforme basis voor zowel risico's, zekerheden, maatregelen én wederzijdse beïnvloedingen. Immers, zij zijn alle uit te drukken in acties (oorzaken en gevolg), kansen van optreden en (financiële) impact. Dit alles zou er in de praktijk uit kunnen zien als in het voorbeeld in het kader.

Voorbeeld

De organisatie CoPie verzorgt de back-up en recovery van data van twee verschillende netwerkservers binnen uw bedrijf. CoPie heeft daartoe binnen uw organisatie een aparte dataserver staan waarop de back-ups geautomatiseerd worden aangemaakt. Service en beheer is geregeld via een SLA.

Een IT-auditor met kennis van complexiteitsanalyses krijgt van u de opdracht om de betrouwbaarheid en continuïteit van het back-upproces te onderzoeken. De auditor voert samen met u een risicoanalyse uit en rapporteert daarna in termen van afhankelijkheden en kwetsbaarheden. Ook stelt de auditor een aantal extra maatregelen voor: M1 t/m M6. U vraagt natuurlijk ook aan de auditor of daarmee de gewenste zekerheid daadwerkelijk wordt bereikt. De auditor stelt u een aantal aanvullende vragen om vast te stellen wat u onder de gewenste zekerheid verstaat. Uit dat gesprek volgt ook dat gevolgen G1 t/m G3 nooit mogen optreden (het elimineren van ongewenste onzekerheden). De auditor rapporteert op basis van analyses aan u het volgende:

'Gegeven de huidige situatie bij CoPie alsmede de scope van het onderzoek kan ik u het volgende mededelen: met een zekerheid van 98% is de maximale financiële impact in het back-upproces op jaarbasis € 2.500. Voor het restrisico van 2% geldt het totaal van de ingeschatte impacts, te weten € 108.000 per jaar. Daarmee is de te verwachten financiële impact € 4.610 (= 98% * 2.500 + 2% * 108.000). De implementatie van de SOLL vermindert het risico derhalve van ruim € 108.000 tot onder de € 5.000. Tevens zullen de door de auditor aangegeven en gespecificeerde schadelijke gevolgen G1 t/m G3 niet op kunnen treden bij het invoeren van de geadviseerde maatregelen (98%). In de bijlage staat de onderbouwing van deze uitspraak.'

U kunt nu als opdrachtgever zelf relatief eenvoudig bepalen of dit totaalrisico voldoet aan uw gewenste (on)zekerheid. Maar u weet inmiddels dat maatregel M4 waarschijnlijk niet past bij uw organisatiecultuur. U geeft aan die maatregel niet uit te kunnen voeren en vraagt daarom aan de auditor om aan te geven wat er in dat geval met de zekerheid en de impact gebeurt. De auditor past daarop zijn analyse aan met de nieuwe gegevens en rapporteert u vervolgens respectievelijk 71% en € 27.000. Daarmee neemt op basis van dezelfde rekenwijze de te verwachten financiële impact toe tot

Tabel 1. Twee denkwerelden

	Zekerheid is een resource	**Onzekerheid is een resource**
Het auditobject…	… wordt gezien als een groot geheel dat tot in de kleinste details kan worden beschreven en geanalyseerd. Door een juiste analyse is het gedrag van dat object als geheel voorspelbaar. Door de beheersmaatregelen op die analyse aan te sluiten is de gewenste beheersing en zekerheid voorspelbaar.	… bestaat uit autonome deelobjecten die relaties met elkaar aangaan. Door het zorgdragen voor juiste relaties en afspraken tussen die objecten is het gedrag van het auditobject voorspelbaar. Door de beheersmaatregelen op die relaties en afspraken aan te sluiten, is de gewenste beheersing en de ongewenste onzekerheid voorspelbaar.
De beheersing is…	… topdown. Control is centraal belegd op een voldoende hoog niveau. De monitoring is gekoppeld aan de centrale aansturing en de beheersing.	… bottom-up (zelfordening). Control is decentraal belegd op een voldoende laag niveau. De monitoring is gekoppeld aan de lokale aansturing (per deelobject).
Maatregelen voor de beheersing…	… zijn gebaseerd op de identificatie van en het verzamelen van informatie over gewenste zekerheden. Maatregelen krijgen hun beslag in algemeen geldende procedures, afspraken en regelgeving.	… zijn gebaseerd op de identificatie van het verzamelen van informatie over ongewenste onzekerheden bijvoorbeeld met een scenarioanalyse. Maatregelen resulteren in flexibele afspraken en relaties tussen deelobjecten.
Er wordt primair gezocht naar…	… complexiteitsreductie door vermindering objecten, relaties, veranderingen, beïnvloedingen et cetera.	… complexiteitsbeheersing door goede afspraken en relaties tussen (deel)objecten.
Het gevoel en verstand op lokaal niveau…	… wordt – vanuit de centrale gedachte dat alles controleerbaar, voorspelbaar en analyseerbaarheid is – verdrongen.	... is door het maken van goede afspraken en relaties juist aanwezig. De lokale creativiteit blijft daardoor behouden. Verder blijft door het autonome van de objecten de flexibiliteit van het geheel ook behouden.
Primair gericht op het…	… 'domein van invloed'; zekerheid wordt bereikt door die dingen te doen die je (centraal) kunt regelen. Aanpassingen worden als gevolg van contextwijzigingen reactief doorgevoerd.	… 'domein van betrokkenheid en acceptatie'; onzekerheid wordt geëlimineerd door afspraken te maken tussen deelobjecten onderling. Aanpassingen worden als gevolg van te verwachten contextwijzigingen proactief voorbereid.
Control in de toekomst…	… wordt gevormd door beheersmaatregelen gebaseerd op ervaringen uit het verleden, toekomstverwachtingen en feiten uit het heden.	… gebaseerd op toekomstverwachtingen en de flexibele structuur van de autonome objectdelen met daartussen afspraken en een basis van vertrouwen (relaties).
Denkwereld is…	… regelgeoriënteerd.	… principegeoriënteerd (net als bijvoorbeeld de Corporate Governance code's).
Complexiteit is inzichtelijk te maken vanuit de aanname dat alle deelobjecten...	… samen als één geheel tot in alle details te analyseren zijn. Een vastlegging van de objectbeheersing (bijvoorbeeld met een algehele AO/IC-beschrijving) is een noodzakelijkheid voor het gewenste inzicht.	… los te analyseren zijn en dat het geheel te analyseren is door de afspraken tussen de verschillende deelobjecten daarbij te betrekken en in scenario's uit te zetten. De deelobjecten zijn vervolgens aanvullend te analyseren op de 'klassieke' manier.

€ 50.490 per jaar. De maatregel is blijkbaar van cruciaal belang op het geheel. Omdat u maatregel M4 echt onhaalbaar acht, weet u nu dat u op zoek moet gaan naar één of meerdere compenserende maatregelen (omdat de toegevoegde waarde van die maatregel € 50.490 – € 4.610 = € 45.880 vertegenwoordigt, dat is ruim 42% van het totaal van de ingeschatte impacts zijnde € 108.000 per jaar). Immers, bij het niet implementeren van M4 accepteert u mogelijk te veel ongewenste onzekerheid.

Maar omdat u ook graag wilt weten wat er met al deze zekerheden gebeurt in een aantal andere scenario's, maakt de auditor samen met u een meer uitgebreide analyse. De volgende waarschijnlijk geachte scenario's worden voor verdere analyse gekozen:

1. standaard, conform onderzoek tot nu toe;
2. als 1, maar met de aanname dat risico R1 niet optreedt (= een aanpassing van het risicoprofiel);
3. als 1, maar waarbij de auditor de twee netwerkservers vervangt door één groter exemplaar (= een aanpassing van het auditobject).

Samen met de auditor bepaalt u alle gegevens voor een uitgebreide analyse waarbij:

1. per scenario en per maatregel de bijdrage in de zekerheid wordt bepaald (net zoals hiervoor met M4 de bijdrage op 42% is bepaald);
2. per (on)zekerheid een inschatting wordt gemaakt van de kans op falen (net zoals hiervoor voor G1 t/m G3 de kans op falen op 2% is bepaald);
3. per risico een inschatting van de kans op optreden wordt bepaald en de daarbij verwachte (financiële) impact per scenario wordt berekend.

Uit die analyse blijkt dat maatregel M4 in alle scenario's een bijdrage in de zekerheid heeft van rond de 40%. De auditor adviseert u derhalve die maatregel toch te implementeren of te zorgen voor een goed alternatief.

Dit voorbeeld laat zien dat de auditor afhankelijk van mogelijke scenario's kan werken met verschillende zekerheden en onzekerheden (een scenario op zich is al een onzekerheid). De gegevens uit de analyse zal de auditor gebruiken ter onderbouwing van de geleverde gewenste zekerheid bij de audit. Immers, uit de onzekerheden in scenario's vloeien de (beheers)opties voor het in control brengen en houden van het auditobject. De opgebouwde kennis kan bij elk volgend onderzoek verder worden uitgebouwd en worden aangepast aan de actuele situatie en gewenste scenario's.

Of, in het algemeen, door de huidige en alternatieve vormen van de beheersing van het auditobject te relateren aan mogelijke toekomstbeelden ontstaat een analysemodel waarvan de uitkomsten kunnen worden gebruikt voor verbetervoorstellen in die beheersing. Zoals dit voorbeeld aangeeft is er een evaluatiefunctie nodig welke aangeeft wanneer een beheersing beter 'fit' bij de gewenste doelstellingen. Die evaluatiefunctie is in het voorbeeld beperkt tot de gemoeide kosten en een soort kansverdeling daarbij. Om de analyse zinvol te maken, zal uiteindelijk iemand op basis van de resultaten een besluit moeten kunnen nemen.

Er zijn ook andere voorbeelden van evaluatiefuncties die mogelijk kunnen worden gebruikt. Immers, waarom alleen maar de impact bepalen aan de hand van de financiële gevolgen? Heylighen [HEYL04] doet op p. 63 van 'Complexiteit en Evolutie' in een vergelijkbare omgeving, namelijk die van een groter aantal samenhangende componenten, een voorzet voor een evaluatiefunctie op basis van de statistische entropie; dat is een maat voor de aanwezige onzekerheid gebaseerd op de kansverdelingen van de toestanden waarin dat geheel zich kan bevinden. Het minimaliseren van die statistische entropie is een voorbeeld van een andere evaluatiefunctie.

Er is hier nog niet beschreven hoe vanuit beide geschetste denkwerelden de complexiteit daadwerkelijk moet worden bepaald. Met de laatste regel in tabel 1 hoop ik echter duidelijk te hebben gemaakt dat de gegevens daarvoor wel voorhanden zijn. Het is aan de auditor om deze tot in alle details uit te schrijven of om af te gaan op goed onderbouwde aannames en schattingen. Verder bestaat de exercitie uit het uitwerken van de mogelijke scenario's, het kiezen en toepassen van de evaluatiefuncties en het analyseren van de resultaten. Simulaties van scenario's kunnen daarbij ook helpen; de scenarioanalyse als tool voor de auditor. De analyseresultaten daarvan zijn mogelijk de basis voor andere beheerskeuzes. Zie bijvoorbeeld maatregel M4 uit het voorbeeld die uiteindelijk in alle onderzochte scenario's van groot belang blijkt te zijn.

Slotwoord

We denken veel in gewenste zekerheden en nog relatief weinig in ongewenste onzekerheden; echter de wereld om ons heen bevat steeds meer onzekere factoren. Onzekerheid is een zekere factor geworden waarmee rekening moet worden gehouden. Er zitten echter grenzen

aan het voorspellen van zekerheid als alleen rekening wordt gehouden met bekende risico's. In meer complexe situaties zullen ook ongewenste onzekerheden een rol gaan spelen bij het in control houden van die situatie.

Door verschillende scenario's naast elkaar te leggen, kan het potentiële resultaat van een set maatregelen nu en in de toekomst nader worden geanalyseerd. Om te bepalen welk (deel van een) scenario beter 'fit' dan een andere is een evaluatiefunctie nodig; daarvan zijn er verschillende bekend waarvan 'de financiële impact' de meest bekende is. De voorspelbaarheid van de beheersing van complexe veranderlijke situaties wordt door het verkregen inzicht groter.

Ik meen dan ook te kunnen zeggen dat een scenario-analyse extra inzicht kan verschaffen in situaties waarin we te weinig zicht hebben op de afhankelijkheden. De term complexiteitsanalyse heb ik gebruikt voor situaties waarbij analysetechnieken tevens de impact van risico's op die scenario's meer inzichtelijk maken. Het voorbeeld op p. 7 demonstreert dat. Resumerend, complexe situaties vertroebelen het zicht op afhankelijkheden en kwetsbaarheden. Scenarioanalyses werken verhelderend voor de vertroebelde afhankelijkheden en complexiteitsanalyses doen hetzelfde voor de vertroebelde kwetsbaarheden. Het totaal van dat alles kan de auditor helpen meer zekerheid te verkrijgen of de voorgestelde set maatregelen (SOLL) nu en in de toekomst toereikend is.

De auditor moet dus blijven zoeken naar gewenste zekerheden, maar doet er goed aan ook expliciet aandacht te schenken aan de eliminatie van onzekerheden. Door het analyseren of zelfs simuleren van scenario's kan hieraan een invulling worden gegeven.

Momenteel ben ik bezig met de ontwikkeling van een toolkit voor genoemde complexiteitsanalyses. Deze is gebaseerd op simulaties van verschillende scenario's en risicoprofielen. Dergelijke simulaties sluiten aan bij de mogelijkheden die zijn geschetst in het voorbeeld. Door het uitvoeren van die simulaties kan blijken of de gemaakte afspraken (zie tabel 1) een juiste uitwerking kunnen hebben. Of die toolkit er uiteindelijk ooit komt is onzeker.

Literatuur

[EDP01] Handboek EDP auditing (2001), op CD-ROM, Kluwer.

[GLEIM01] Gleim, I.N. (2001), *CIA Review*, part I, 10de editie, Internal Audit Proces (de gebruikte definities van risico en maatregel zijn – vrij vertaald – hieruit overgenomen).

[HERR02] Herrera R. en A. Omar (2002), *Graphical Risk Analysis (GRA): A Methodology To Aid In Modeling Systems For Information Security Risk Analysis,* Deloitte & Touche, Mexico.

[HEYL04] Heylighen, F. (2004), *Complexiteit en Evolutie*, cursusnota's 2003-2004, centrum Leo Apostel, Vrije Universiteit Brussel, vrij beschikbaar op http://pespmc1.vub.ac.be/CLEA/CompEvCursus.html.

[KELLY94] Kelly, K. (1994), *Out of Control, The new biology of machine,* Fourth Estate, Londen, UK.

[MOS98] Mos, T. (1998), Het (accountants?) audit-risk voor IT-auditing beschouwd, in: *de EDP-auditor,* nr. 3, pp. 4-15.

[PIJL00] Pijl, G.J. van der (2000), IT-auditing in a changing world, Inaugurele rede, in: *de EDP-auditor*, nr. 4, pp. 37-40.

[ROBB02] Robbers, R.M.R. (2002), *Complexiteitsanalyse, een aanvulling op de risicoanalyse voor de IT-auditor*, referaat postdoc. EDP-auditing aan de EUR.

[TRUIJ96] Truijens, J. en J. Winterink (1996), Complexiteitstoename van de (geautomatiseerde) informatieverzorging, in: *de EDP-auditor*, nr. 3, pp. 3-14.

[VIR94] Voorschrift Informatiebeveiliging Rijksdienst (1994).

[VIR98] NGI (Nederlands Genootschap voor Informatica), Afdeling Beveiliging (1998), onder redactie van J. Bautz en C. Schonfeld, *Vier jaar VIR, vloek of zegen?*, Ten Hagen Stam.