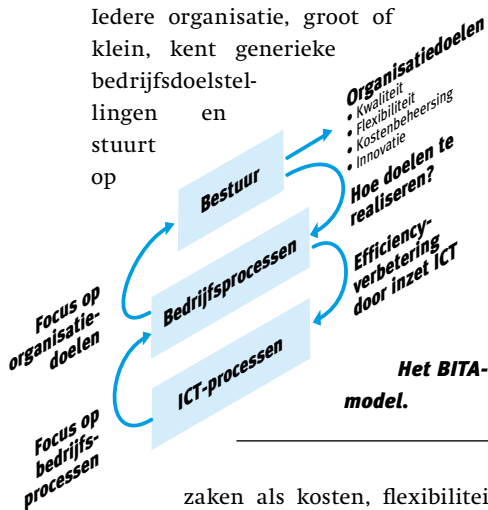


Rampen zijn niet te plannen, maatregelen wel

De continuïteit van ICT-diensten is tegenwoordig zeer belangrijk. Dit artikel gaat in op de organisatorische en procesaspecten bij bedrijfscontinuïteit. Een goed doorlopen continuïteitsplan kan uiteindelijk bij onverwachte calamiteiten een goede uitkomst bieden.

Door Aad Brinkman en Peter de Laat

ICT-diensten zijn tegenwoordig binnen de 24-uurseconomie niet meer weg te denken. De komst van IP-telefonie en de integratie daarvan in het datanetwerk heeft de belangrijkheid van deze dienstverlening verder versterkt. Daarbij is dus ook de continuïteit van de ICT-dienstverlening verder toegenomen. Om het belang van deze continuïteit goed te kunnen begrijpen, moeten bedrijven en organisaties zich in de eerste plaats afvragen waarom zij hun ICT-diensten, inclusief de telefonie, juist willen continueren. Een *Business-IT Alignment* (BITA)-model laat zien dat ICT-oplossingen de bedrijfsprocessen ondersteunen. Iedere organisatie, groot of klein, kent generieke bedrijfsdoelstellingen en stuurt op



zaken als kosten, flexibiliteit, innovatie en kwaliteit. Om aan de behoefte van de klanten of afnemers te

voldoen, zijn er afdelingen die voor de uitvoering van de bedrijfsprocessen zorgen. Deze bedrijfsprocessen worden zo effectief en efficiënt mogelijk geleverd conform een afgeleide doelstelling van de bedrijfsdoelstellingen. De ICT-diensten, die door ICT-afdelingen worden geleverd, moeten op hun beurt weer bijdragen aan de effectiviteit en de efficiency van deze bedrijfsprocessen. Steeds meer ICT-afdelingen richten hun beheer in volgens bekende raamwerken, zoals *Information Technology Infrastructure Library* (ITIL), *Open Service Management Framework* (OSMF), *Control Objectives for Information and related Technology* (COBIT) en ISO 2000 voor beheerprocessen. Eén van die processen, ICT-continuïteitsbeheer, moet voor de continuïteit van ICT-diensten, inclusief telefonie, zorgen. Dat dit allemaal dient om een bijdrage aan de bedrijfsprocessen te leveren, is voor veel ICT-organisaties nog vrij nieuw, of beter gezegd, wordt pas sinds een paar jaar onderkend en komt tegenwoordig terug onder de noemer *IT-governance*.

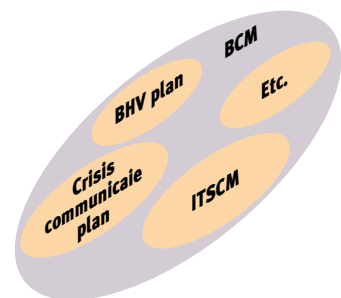
ITSCM

IT-governance is tegenwoordig weer zeer actueel. Nog geen 10 jaar geleden bestond binnen de eerste versie van ITIL het proces *Contingency Planning*. Dit proces stond tamelijk op zichzelf en produceerde een uitwijkplan waarmee de ICT-afdeling in geval van calamiteiten de infrastructuur snel weer operationeel zou moeten krijgen. Als deze plannen eenmaal klaar waren, verdwenen ze in een kast en werd er niet meer naar omgekeken. Door het millenniumprobleem en de gebeurtenissen op 11 september

2001 kwam het continuïteitsproces in een nieuw daglicht te staan. Begin deze eeuw, bij de introductie van de tweede versie van ITIL, werd het proces tot *IT Services for Continuity Management* (ITSCM) omgedoopt. Het proces werd een integraal onderdeel van *Business Continuity Management* (BCM). Dit was een belangrijke stap voorwaarts omdat daarmee de continuïteit van de ICT-diensten direct aan het doel, continuïteit van de primaire processen van organisaties, werd gekoppeld.

ITSCM gaat er van uit dat ook de businesskant na moet denken over hun eigen continuïteit. Die heeft een eigen verantwoordelijkheid. De businesskant kan niet blind varen op de ondersteuning door de ICT-afdeling of de andere ondersteunende diensten. De businesskant moet zich daarom ook afvragen wat er gedaan moet worden als gas, water of energie uitvallen, wie de klanten moet bellen na een brand of hoe het met de veiligheid van het personeel, het BHV-plan, zit.

ITSCM heeft hiermee aan kracht en belang gewonnen en kan daadwerkelijk bijdragen aan een van de primaire doelstelling van de organisatie, de continuïteit van diensten voor klanten en personeel. De BCM-standaard BS25999 geeft richtlijnen en zelfs de mogelijkheid om het BCM-proces te certificeren.



De planning van de businesskant in combinatie met ITSCM.

Aad Brinkman (a.brinkman@apreton.nl) en Peter de Laat (p.d.laat@apreton.nl) zijn respectievelijk Principal Consultant en senior consultant bij Apreton.

Het ITSCM-proces kent vier fases, een initiatie, strategie-, implementatie, en operationeel beheer. De fases zijn onafhankelijk van onder meer het ITILv2-, ITILv3-, NIST-, COBIT-, OSMF-raamwerk en zijn altijd te onderscheiden. In de initiatiefase vindt een duidelijke afbakening van het algemene kader plaats tussen de verschillende disciplines binnen het BCM. Naast de afbakening van het algemene kader, is het zeer belangrijk om de taken, rollen, verantwoordelijkheden en bevoegdheden binnen de verschillende onderdelen vast te stellen. Daarna kan, in samenwerking met de businesskant, voor de verschillende onderdelen beleid worden ontwikkeld.

Strategiefase

Om de continuïteit van de ICT-diensten efficiënt te kunnen waarborgen, is het van belang om vervolgens te onderzoeken welke bedrijfsprocessen echt essentieel zijn voor de continuïteit van een organisatie en op welke wijze deze door ICT worden ondersteund. Dit vindt plaats in de strategiefase. Dit onderzoek moet de ICT-afdeling in samenwerking met het businessmanagement verrichten.

ICT-continuïteitsbeheer is essentieel

te verkrijgen. Bij het onderzoeksinstituut zijn telefonie en ICT volledig in het primaire bedrijfsproces geïntegreerd. De continuïteit van deze geïntegreerde dienst is daardoor van levensbelang voor de voortbestaan van de organisatie. Het tweede voorbeeld is een grote internetwinkel. Bij deze online winkel is telefonie van ondergeschikt belang en eigenlijk alleen bedoeld voor de communicatie van de ondersteunende processen, zoals de inkoop. Toch wordt voor deze processen eigenlijk veel meer e-mail gebruikt. Voor de website zal zonder enige twi-
fel een uitstekende continuïteitsvoorziening

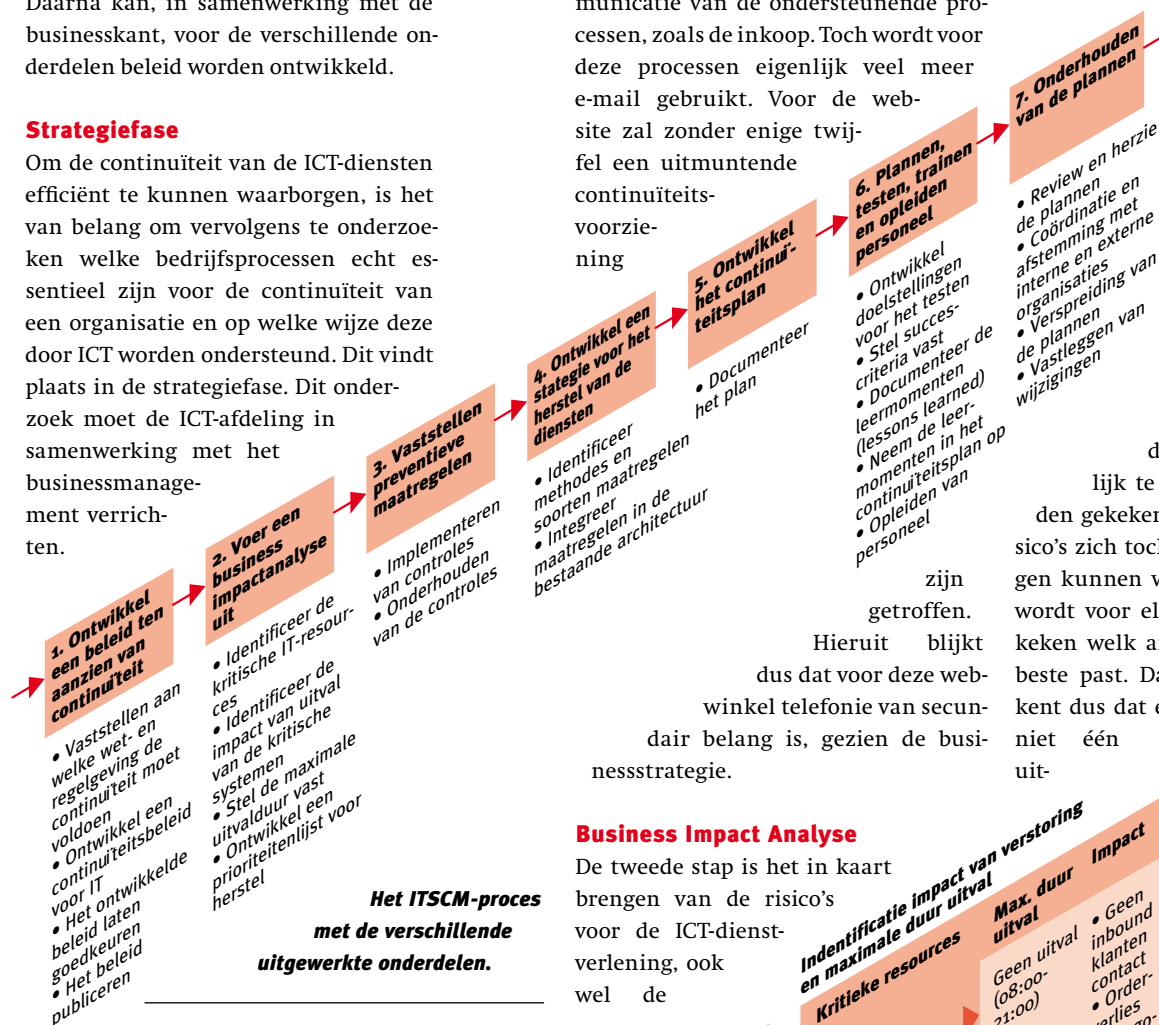
Business Impact Analyse (BIA) genoemd. De vraag hierbij is op welke manier de ICT-voorzieningen door externe of interne bedreigingen kunnen worden geraakt, die de continuïteit van de dienstverlening in gevaar kunnen brengen. Het Amerikaanse National Institute of Standards and Technology (NIST) heeft voor deze analyse een stappenplan opgesteld.

Naast het uitvoeren van de BIA kan een risicomatrix voor het bepalen van de te volgen strategie worden gebruikt. Deze matrix wordt opgesteld aan de hand van de kans op een calamiteit en de impact op de bedrijfsprocessen. Door het overzicht van deze risico's kunnen de juiste tegenmaatregelen worden genomen om de kans op het optreden van

de risico's zo klein moge-

lijk te maken. Daarna kan wor-

den gekeken, voor het geval dat de risico's zich toch voordoen, hoe de gevolgen kunnen worden beperkt. Hierbij wordt voor elk foutscenario gekeken welk antwoord het beste past. Dat betekent dus dat er niet één uit-



Het ITSCM-proces met de verschillende uitgewerkte onderdelen.

Business Impact Analyse

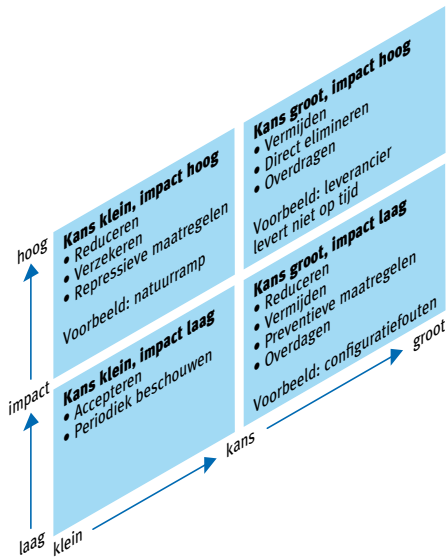
De tweede stap is het in kaart brengen van de risico's voor de ICT-dienstverlening, ook wel de

Twee voorbeelden geven het verschil in belang aan voor de strategie van de organisatie van telefonie. Het eerste voorbeeld is een onderzoeksinstituut dat naast online enquêtes, ook veel telefonische enquêtes voor een ministerie doet. De website en e-mail zijn voor derden de belangrijkste contactpunten om informatie van dit bureau



Het stappenplan van het NIST.

wijksscenario is, maar doorgaans meerdere, afhankelijk van de calamiteit. Welke oplossingen er ook worden gekozen, de krachten-driehoek People, Process, Technology moet wel in balans blijven. Vaak wordt er een technische oplossing bedacht of juist alleen het proces beschreven of alleen de verantwoordelijken aangewezen. Om uiteindelijk succesvol te zijn moet aan alle drie de aspecten in de krachten-driehoek aandacht worden besteed.



De risicomatrix.

	Maatregelen en activiteiten		
	Strategisch	Tactisch	Operationeel
Alarmerings-fase	Herkenning en erkenning	Escalatie en alarmeringsprocedure	Escalatie en alarmeringsprocedure
Activerings-fase	Analyse en besluitvorming	Opstarten BCP	BHV & ontruiming en schade inventarisatie
Uitvoerings-fase	Terugdringen gevolgschade en formuleren herstel strategie	Uitvoering geven aan BCP en managen van de organisatie in uitwijk	Disaster recovery nood procedures, reconstructie en achterstand inhalen
Nazorg en evaluatie	Besluitvorming terugkeer, business as usual, nazorg en evaluatie	Management van de inwijk	Herstel normale operatie

Het stelsel van maatregelen in de implementatiefase.

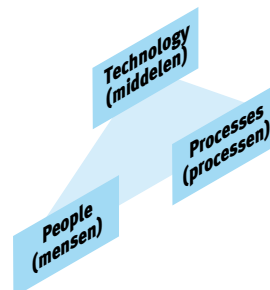
Een voorbeeld. Uit de risicoanalyse blijkt dat door de ligging in de uiterwaarden van een rivier, het grootste risico een overstroming is. Daarnaast wordt brand niet uitgesloten. Door ervaring wijs geworden, weet een bedrijf dat ook stroomuitval een probleem kan zijn. De tegenmaatregelen zijn vervolgens een noodstroomvoorziening en een goede blusinstallatie in de serverruimte. Dit zijn beide technische oplossingen. Ook aan de proceskant is gedacht. Een overstroming valt te voorspellen. Het antwoord hierop is door in de uitwijkplannen een scenario op te nemen dat uitgaat van een snelle verhuizing van de servers. Bij brand treedt een ander scenario in werking. Een uitwijkcontract zorgt dan voor ICT-voorzieningen op een andere locatie. Natuurlijk worden ICT-medewerkers en personeel getraind voor beide si-

Continuïteitszorg evolueert naar doordacht proces

tuaties. Op de uitwijklocatie wordt minimaal één keer per jaar uitvoerig getest. Ook het *change*proces is onder de loep genomen. Een wijziging op de infrastructuur kan namelijk effect hebben op de eerder vastgestelde scenario's.

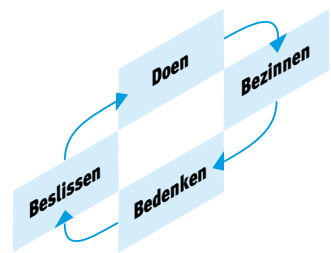
Implementatiefase

Uiteindelijk moeten de technologische oplossingen, samen met de processen en de toewijzing van verantwoordelijkheden, ertoe leiden dat er op alle niveaus binnen de organisatie draaiboeken klaarliggen voor het moment van escalatie. De implementatie en borging van deze maatregelen vinden plaats in de derde fase van het proces, de implementatiefase.



De krachtendriehoek.

Binnen deze fase worden de initiële plannen voor de uit- en inwijk opgesteld en getest. Het is van het grootste belang dat personeel wordt opgeleid en dat het testen wordt gebruikt om de succesfactoren vast te stellen. De *lessons learned* moeten worden verwerkt in het uiteindelijke plan. De *leercirkel van Kolb* kan hierbij een houvast zijn. Neem altijd de tijd om te bezinnen. Wat is er aan de hand? Bedenk vervolgens de mogelijke oplossingen en beslis vervolgens. Dit is de stap waarin de oogst van het hele proces wordt binnengehaald.



De leercirkel van Kolb.

Operationeel beheer

De laatste fase is het operationeel beheer van alle zaken die bedacht en opgeschreven zijn. In feite moeten bedrijven en organisaties nu precies weten wat er moet gebeuren in geval van calamiteiten. Het houdt dus niet op bij het alleen maken van plannen. De processen en alles wat daarmee samenhangt, moeten actueel en afgestemd blijven op de juiste ondersteuning van de continuïteit van de veranderende bedrijfsprocessen. Als de klanten van een organisatie veranderen, en dat doen ze geregeld, zullen er andere eisen aan de ICT moeten worden gesteld. Dat betekent een aanpassing van de bedrijfsprocessen en dus wellicht ook een verandering van de ICT-ondersteuning. Dan moet ook de ICT-continuïteit daarop worden aangepast. Dat kan een aanpassing zijn van de procedures en misschien andere technische tegenmaatregelen. Uiteraard zal ook het personeel hierbij weer moeten worden betrokken en getraind. De continuïteitszorg is geëvolueerd van het maken van uitwijkplannen tot een gedegen en doordacht proces. Een belangrijke succesfactor voor het operationeel beheer is een goed wijzigingsbeheer over de complete set van plannen. De kwaliteit van dit wijzigingsbeheer kan worden afgemeten aan de frequentie waarmee de plannen wordt bijgewerkt, in relatie tot de dynamiek van de betreffende organisatie. Hoe dynamischer de organisatie, hoe vaker de plannen, met behulp van het proces voor wijzigingsbeheer, zullen veranderen. ■

Literatuur

- BCM Pocketbook, L. Knegtel, BCM Academy, Harderwijk
- ITIL V2, Service Delivery, OGC, TSO 2003,
- ITIL V3, Service Design, OGC, TSO 2007
- NIST, NIST special publication 800-34, *Continuity Planning Guide for Information Technology Systems*, M. Swanson et al, U.S. Department of Commerce, 2002

Conclusie

De continuïteit van ICT-diensten, inclusief telefonie, is essentieel voor het voortbestaan van vrijwel alle organisaties. Hier kan dus niet al te lichtzinnig over worden nagedacht. Een gedegen voorbereiding en het beschrijven van de juiste scenario's kan een hoop slapeloze nachten schelen.