Klanten willen vooral wendbaarheid

KIJK OP EN OMGAAN MET IT-RISICO

Anno 2009 is ICT voor onze organisaties van vitaal belang geworden. Optimale inzet van ICT kan de wendbaarheid vergroten, zonder juiste sturingsgegevens is er geen optimale besluitvorming, het kunnen tracen van activiteiten leidt tot minder misbruik. Daarom moet de ICT maximaal en optimaal beschikbaar zijn. Dit artikel kijkt eerst, vanuit de bril van de manager van de klanten van ICT, naar hun besef van het risico, dat zij lopen met de afhankelijkheid van ICT. Hoe denken die klanten over het risico, dat ICT op enig moment niet beschikbaarheid is? Of dat het gebruik van ICT niet voldoende beschermd is? De gegevens niet goed genoeg zijn, of de steun die de ICT biedt niet adaptief genoeg?Vervolgens bespreekt het de maatregelen, die een organisatie kan nemen om deze risico's zo veel mogelijk te beperken.

DOOR THEO THIADENS C.S.

In de negen organisaties die het object vormden van het hieronder beschreven onderzoek wordt de beschikbaarheid niet echt als een probleem ervaren. Bescherming van data verdient duidelijk meer aandacht; managementinformatie moet in sommige organisaties nog een groeipad doormaken, en aan een grotere wendbaarheid van de ICT dient prioriteit te worden toegekend. Wat betreft de maatregelen om het risico te beperken, kan worden geconstateerd, dat de negen organisaties alle willen werken onder architectuur, om te komen tot een grotere mate van standaardisatie van ICT-voorzieningen. Ook kan worden geconstateerd, dat organisaties risicomanagement niet als een separate functie hebben georganiseerd. Evenmin is er eenduidigheid qua methoden om de risico's te bepalen. Bewustzijn van de risico's was wel binnen elk van de organisaties aanwezig.

Inleiding

Organisaties zijn steeds afhankelijker geworden van de inzet van ICT. In sommige organisaties is het leveren van producten en diensten zonder ICT in de laatste vijftien jaar zelfs onmogelijk geworden. Beschikbaarheid van ICT wordt zo een levensbehoefte voor het management – dat dan ook prioriteiten moet stellen. Wil men een maximale beschikbaarheid van ICT? Eist men 100% bescherming, bij het gebruik van de ICT? Zou het management, indien het kon beschikken over betere gegevens, ook beter kunnen inspelen op de wensen van de klant? Welke risico's is men bereid daarbij te lopen? Het management moet afwegingen maken. Het kan een accent leggen op beschikbaarheid van ICT, op bescherming bij gebruik van ICT, op accuraatheid van gegevens of op verhoging van de wendbaarheid door inzet van ICT.

In het afgelopen voorjaar is onderzoek verricht naar welke prioriteiten managers van organisaties leggen, qua acceptatie van risico bij het gebruiken van ICT. En wat organisaties doen om aan de eisen van deze prioriteiten tegemoet te komen.

Dit artikel geeft een korte samenvatting van de voornaamste resultaten van dit onderzoek. Het artikel gaat eerst in op de methode van onderzoek. Vervolgens geeft het artikel de resultaten van het onderzoek weer. Hierbij wordt eerst ingegaan op de risico's, die managers aan de gebruikerskant bij inzet van ICT zien; daarna wordt globaal aangegeven, welke maatregelen organisaties hebben genomen om de risico's wat betreft de inzet van ICT te minimaliseren.

De theorie achter het onderzoek

Vanuit een organisatie gezien kan ICT-risico (Westerman c.s., 2007) worden gedefinieerd als de mogelijkheid dat een

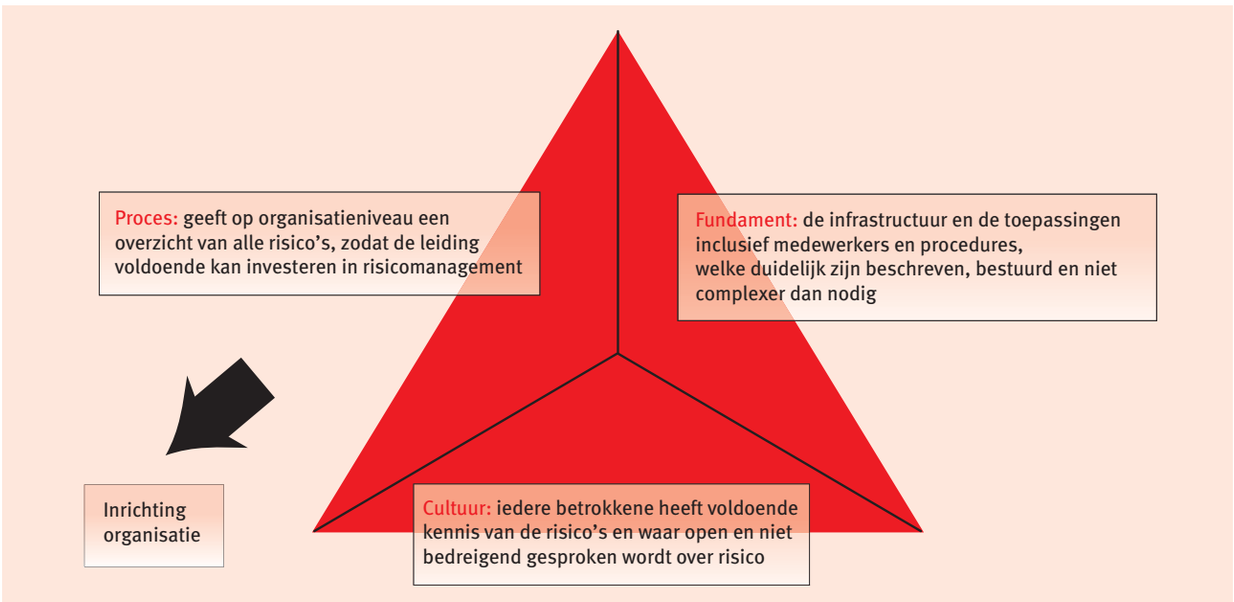
ongeplande situatie optreedt, welke direct te maken heeft met het gebruik van ICT. Bij inzet van ICT loopt een organisatie risico's op vier vlakken, de zogenaamde 4A's. Deze vier A's zijn:
Availability: het ***beschikbaar hebben*** van de nodige ICT en het snel kunnen herstellen van onderbrekingen;
Accessibility: het ***toegang krijgen*** tot gegevens en applicaties op een zodanige wijze, dat de juiste mensen de applicaties kunnen gebruiken en onbevoegden worden geweigerd;
Accuracy: het ***volledig en op tijd beschikbaar hebben*** van de gegevens, zodat aan de eisen van de leiding, de staf, de klanten, de leveranciers en de wetgever kan worden voldaan;
Agility: het bieden van de mogelijkheid om de ICT ***op beheerste wijze te veranderen****.* Dit kan noodzakelijk worden bij een reorganisatie, een fusie, bij een nieuw procesontwerp of bij de lancering van een nieuw product.

Organisaties nemen maatregelen om met deze risico's om te gaan. Die maatregelen kan men weer indelen in drie soorten, zo blijkt uit het onderzoek van Westerman bij 180 grote bedrijven. Het gaat om de zorg voor transparantie van ICT-voorzieningen, het zorgen voor een besef van gelopen en te lopen risico's bij medewerkers, en het organiseren van aandacht voor risicomanagement.
Omgaan met ICT-risico's betekent, dat organisaties kijken naar het totale risico en afwegingen maken ten aanzien van de te nemen maatregelen (zie figuur 1).

Dit leidt in het algemeen tot:
a een meer transparante inrichting van de **ICT-voorziening**.
Met andere woorden, een transparante architectuur van producten en diensten, geleverd door een adequaat beschreven ICT-organisatie. De voorzieningen en de organisatie zijn niet complexer dan nodig;
b de aanwezigheid van een **organisatie voor risicomanagement**, die ervoor zorgt, dat op het niveau van de organisatie een overzicht aanwezig is van de bestaande risico's. Hierdoor is de leiding in staat voldoende tijd en middelen te investeren in risicomanagement. In dit risicomanagementproces worden risico's geïdentificeerd, van een prioriteit voorzien en gevolgd;
c **een cultuur**, welke ervoor zorgt, dat iedere betrokkene voldoende kennis heeft van de risico's en ermee rekening houdt (risk awareness). In deze cultuur wordt open en niet bedreigend gesproken over mogelijk te lopen risico's.

De resultaten van het onderzoek

De maatregelen, die organisaties nemen om het risico van de inzet van ICT te beperken, werden onderzocht met behulp van diepte-interviews. Deze interviews werden gehouden met managers en medewerkers, die vaak een leidende rol spelen in hun organisatie. Er werden standaardvragenlijsten gebruikt, die tevoren aan de negen organisaties werden toegestuurd. De vragen voor de interviews werden geformuleerd door de kenniskring van het lectoraat. Hierbij vormde de theorie van Westerman (2007) de basis. Per organisatie werd aan de kant van de gebruikers en aan ICT kant een interview afgenomen. De geïnterviewde personen werkten in de volgende organisaties: Fontys Hogeschool, de chip producent NXP Semiconductors, De Hypotheker, het Amphia ziekenhuis, de verzekeraar Achmea, het Centraal Justitieel Incas-



Figuur 1
Types maatregelen om risico te verkleinen

Onderwerp:	Beschikbaarheid:		Bescherming:	Nauwkeurigheid, tijdigheid & betrouwbaarheid van gegevens:	Agility:
Organisatie	Hoe vaak uitgevallen in laatste 12 maanden?	In staat schade te beperken?	Op welke wijze toegang?	Belangrijkste data beschikbaar?	Hoe vaak overschrijden projecten met ICT geplande tijd of budget?
Fontys	Unplanned downtime 1,5 dag uitval van sharepoint, naast gepland onderhoud	Er wordt van uitgegaan dat dat alles werkt, anders handmatig	Password en logon tot hele omgeving	Ja, kan altijd over worden beschikt. Inzicht in vrije leslokalen behoeft verbetering	50% uitloop in budget en tijd bijprojecten
Amphia	Twee á drie keer per maand alleen deelsysteem;	Ja, uitval is van korte duur	Inloggen met naam/password	Patiëntgegevens zijn er; mangementinfo ontbreekt	Bijna altijd schattingen te laag
Achmea	Niet eenmaal	Direct gaat calamiteitenplan in	Naam/password én alles gelogd	Ja, 7 maal 24 uur	Bijna altijd
NXP	Verschilt per applicatie en locatie. Root cause analyse in alle gevallen verplicht	Ja, uitwijk & continuïteitsplan	Profielen en aanvragen via baas	Ja, voor operationele gegevens wel	Soms, recent ingevoerde projectmanagmentmethodiek helpt dit te monitoren
Hypotheker	Een keer een uur	Ja, er is uitwijk; max. 24 uur down	Naam/password op persoon	Werkt op basis actielijst niet afwerken niet ontdekt	Alleen installatie bij stabiliteit appl.
IB-Groep	Communicatie met scholen viel vorig jaar uit	Er is een uitwijkcentrum	Via naam/password	Ja, rond 98%. Niet alle gegevens ook altijd op tijd binnen van klant	Vaak, reden: begin schatting project te laag
Kadaster	Eenmaal, maar alleen deelsysteem. Onmogelijk dat alles down is	Uitwijk beperkt dit. Handmatig is onmogelijk	Wordt gewerkt aan profielen. Nu naam/password	Middels workflowmanagementsysteem voor het halen van de termijnen	Vaak, ook al gebruiken we Prince-2
Politie	Niet ter beschikking zijn zelden, papieren back-up	Processen hebben lager niveau	Via profielen	Ja, voor operationele data; Managementinfo niet altijd	40-50%
CJIB	Niet eenmaal	Normaal via de ITIL-processen, anders business-continuïteitsplan	Via naam en password	Ja, 9 systemen met een beschikbaarheid van 98,9%	Soms

Figuur 2

Weergave van enige aspecten van IT risk, bezien vanuit de gebruikers van ICT

sobureau (CJIB), de IB-Groep, het Kadaster en de Politie. Proefinterviews voor dit onderzoek werden gehouden binnen Fontys Hogeschool ICT en de Fontys ICT Services afdeling. Alle onderzochte organisaties hebben meer dan 1400 medewerkers.

Resultaten aan gebruikerskant: visie van klant op ICT risico

In figuur 2 is een overzicht gegeven van resultaten van de interviews per organisatie. Duidelijk wordt uit de figuur dat elke leidinggevende weet, wat ICT voor hem betekent. Dat komt al naar voren doordat men gewoon kan aangeven, wanneer de laatste uitval van ICT plaatsvond en wat daarvan de schade was.

Kijkend naar de gegeven antwoorden kan men concluderen, dat in de onderzochte organisaties beschikbaarheid van ICT eigenlijk geen probleem is. Dat is anders bij de bescherming van de ICT. Hier is het gebruik van profielen, die duidelijk aangeven, wat men in een bepaalde rol mag, geen gemeengoed. Ook bleek niet in alle organisaties een complete logging van de handelingen op het systeem plaats te vinden. Kijkend naar de kwaliteit van de informatievoorziening komt naar voren, dat vaak nog winst te behalen valt op het terrein van managementinformatie. Ten slotte wordt geconstateerd, dat het op tijd en op budget opleveren van nieuwe applicaties een unieke gebeurtenis is. De uitloop in tijd en geld, van vaak meer dan 50%, wordt verklaard door enerzijds de gebrekkige schattingen op dat terrein aan het begin van een project, en anderzijds door het feit, dat men pas in productie gaat, als een applicatie volledig stabiel is.

Het verbaast dan ook niet dat, toen gevraagd werd een voorkeur uit te spreken ten aanzien van één van de 4A's, de geïnterviewde managers in zeven van de negen organisaties de voorkeur gaven aan *agility* of wendbaarheid van de ICT. Alleen de adjunctdirecteur van Fontys hogeschool merkte op, dat voor hem ICT gewoon beschikbaar moet zijn, en dat die beschikbaarheid boven alles gaat. Ten aanzien van bescherming merkte een aantal managers voorts op, dat de situatie wel leefbaar moet blijven. In een ziekenhuis bijvoorbeeld kan

men geen arts verplichten af te loggen, als aanloggen weer enige minuten duurt. Inzet van pasjes, irisscan en vingerafdruk zou op het terrein van bescherming het gebruikersgemak kunnen vergroten.

Maatregelen om ICT-risico's te verkleinen

In figuur 3 is een globaal overzicht gegeven van maatregelen, die organisaties nemen om risico's te managen. De maatregelen om te komen tot een zo transparant mogelijk ICT zijn duidelijk. Grotere organisaties, zoals die deelnamen aan dit onderzoek, standaardiseren wat betreft hun inzet van ICT. Deze organisaties hebben soms nog legacy-applicaties, maar deze bouwt men af (de grote overheidsdienst). De organisaties merken voorts op te werken met architecturen, waarin de afspraken voor de inrichting en de objecten zijn vastgelegd. Het valt hierbij op, dat werken met architectuur kennelijk gaat boven het vastleggen van een helder beschreven ICT-beleid.

In de meerderheid van de gevallen is een continuïteitsplan aanwezig, en wordt dit plan ook periodiek gereviewd en getest. Voorts beschikt men overal over gegevens over de beschikbaarheid van ICT.

Gezien de opmerkingen van de managers aan de gebruikerskant is het helder, dat gevraagd naar de waardering voor ICT

Onderwerp:	**ICT maatregeken**					**Organisatie:**		**Awareness**
Organisatie:	Standaardisatiebeleid voor ICT?	Helder ICT-beleid om richting te geven?	Contunuïteitsplan & review policy?	Gegevens beschikbaarheid	Begrijpt organisatie IT?	Hoe is risicomanagement georganiseerd?	Methode voor inschatting?	Besef dat intellectueel eigendom en kennis vitaal is?
Fontys	Standaard is de technische en informatische infra; Appliaties niet, wel voorwaarden	Nee er technische kaders	Nee, na 2010 aanwezig	Ja, 1x per maand rapportage	Exploitatie heeft waardering; projecten ligt moeilijker	Geen apart afdeling of risk officer	Nee	Nee, wel denken aan beschikbaarheid
Amphia	Technisch en informatisch ja. Applicaties minder	Ja, en inkoop past het toe	Nee, in de planning	Ja, maar niet verspreid	Exploitatie ligt goed	Via stuurgroep ICT	Spark sprint	Nog niet echt
Achmea	Technisch ja, overig trend naar	Ja	Ja en eens pj. getest	Ja, 99,8% Rapport/wk	Blijft knellen	Ja, team met risk officers	DICE voor projecten	Ja, er zijn richtlijnen
NXP	Ja, maar minder in productieomgeving	Ja	Ja en eens pj. review	Ja, standaard in contracten	Er is een linking pin per afdeling	Onderdeel ICT-organisatie	ISF.Firm	Ja, binnen project ingebouwd, anders awareness
Hypotheker	Technisch, inf. en qua applicaties	Neen	Ja, en elke 3 mnd update	Rapportage per maand	Deels overleg	Vooral rond projecten	Nee	Ja, binnen ICT zeker
IB-Groep	Technisch en inf. ja, voor applicaties deels	Werkt met architectuur	Ja, en 2x pj. review	Ja, nodig voor opdrachtgevers	Wisselend	In ontwikkeling	Sessies, Cosso, Prince 2	Ja, maar e is geen intellectueel eigendom
Kadaster	Ja, uniforme exploitatie omgeving	Ja, op basis architectuur	Ja, 6x pj. review, 2x test	Ja, pmnd naar klant	Moeilijk punt	Stand-by & calam.mng	Op delen walkthourgh	Ja, bij exploitatie sterk gefocust
Grote overheidsdienst	Ja, voor infra en applicaties	Ja	Twincenters	Ja	Geen mening	Assessment audits, etc.	Via schatten en meten	Ja, speerpunt kennis bijhouden
CJIB	Ja, maar er is nog legacy	Kan explicieter	Ja, 1x pj test & review	Ja, 98,9%	Veel spanning hier	Via projectleiders	CRAMM mtv. VIB	Ja, maar er is een grens

Figuur 3

De maatregelen die een organisatie neemt.

de meningen verschillen. Er zijn organisaties, die stellen dat de exploitatie van ICT in hoog aanzien staat, maar dat hun organisatie voor ontwikkelen en onderhouden van applicaties niet altijd waardering krijgt voor haar werk.
Beleid en maatregelen om risicomanagement als zelfstandige discipline te organiseren staan vaak nog in de kinderschoenen. Alleen bij de verzekeraar is er sprake van een inbedding van een organisatie voor risicomanagement, die rapporteert aan de hoogste leiding van de onderneming. Vaak is het denken over ICT-risico onderdeel van de taak van een afdeling Beveiliging in een ICT organisatie (NXP Semiconductors en Amphia ziekenhuis). Soms is het alleen een onderwerp bij ICT-projecten, zoals bij het CJIB en de IB-Groep, of mist men een methodische aanpak voor het omgaan met risico in de lijn (De Hypotheker). Op het terrein van de methoden die gebruikt worden om ICT-risico in te schatten, komt er een variëteit aan aanpakken naar voren.
Ten slotte de awareness van het ICT-risico. Deze is in elke onderzochte organisatie aanwezig. Open kan intern over risico's worden gepraat. Systematische en formele uitwisseling van ervaringen op dit terrein vindt echter slechts beperkt plaats.

Conclusies
Kijkend naar *IT Risk* is anno 2009 de beschikbaarheid van ICT geen probleem meer. Het omgaan met de bescherming van gegevens en functionaliteiten is een groter punt van zorg. Op het terrein van de kwaliteit van de gegevens lijkt er bij sommige organisaties qua kwaliteit van managementinformatie nog het nodige te winnen. Wat betreft agility wordt duidelijk, dat geen manager nieuwe ICT invoert, als deze niet goed functioneert. Dit is vaak de reden die wordt aangegeven voor budget- en tijdoverschrijdingen.

Fontys merkt voorts op, dat iedere organisatie een ander accent kan leggen wat betreft ICT- risico's. Fontys eist als hogeschool in eerste instantie beschikbaarheid van haar ICT, maar ziet ook dat een betere kwaliteit van gegevens haar werk ten goed zou komen. Op de wensenlijst van de meeste organisaties staat duidelijk de wens naar een grotere wendbaarheid van ICT als eerste prioriteit.

Bij de maatregelen om risico bij inzet van ICT te beperken wordt duidelijk, dat de onderzochte organisaties in hoge mate streven naar werken onder architectuur en dat hierbij in sterke mate wordt gestandaardiseerd. Helder is voorts, dat exploitatie van ICT vaak als een facilitaire dienst wordt gezien. Deze dienst wordt beter gewaardeerd dan het leveren van ontwikkelings- en onderhoudsdiensten. Begrip kweken bij de klant voor deze laatste diensten lijkt niet zonder uitdaging.
Een aparte organisatie voor risicomanagement werd alleen bij de verzekeraar aangetroffen. Bewustzijn van de bij inzet van ICT-risico's lijkt daar, waar nodig, aanwezig.
De slotconclusie kan luiden, dat, naarmate ICT belangrijker wordt, de aandacht van de klanten van ICT wordt gericht op wendbaarheid van de inzet van ICT. De organisaties nemen maatregelen als grotere standaardisatie van ICT en werken onder architectuur. Zij staan aan het begin wat betreft inrichten van een aparte organisatie voor risicomanagement, en moeten inspanningen leveren om awareness van het risico, dat inzet van ICT met zich meebrengt, levend te houden.

- Westerman, G. en R. Hunter, *IT risk, turning business threats into competitive advantage*, Harvard school press, Boston 2007.

De auteurs danken de geïnterviewde organisaties, te weten Achmea, Amphia Ziekenhuis, het CJIB, Fontys hogescholen, De Hypotheker, de IB-Groep, het Kadaster, de Politie, Fontys, NXP Semiconductors en Simac voor hun medewerking aan het onderzoek en dit artikel.