Risicomanagement in een e-businessomgeving

Drs. ing. R.F. Koorn CISA RE, drs. B.H.M. Peters RA en P. Freeborn MSc

Risicomanagement wordt in vele organisaties toegepast, alleen nog niet altijd expliciet gericht op e-businessplanning, -projectuitvoering of het operationeel houden van een e-businessomgeving. In dit artikel wordt ingegaan op een aanpak voor e-businessrisicomanagement, waarbij het gebruik van geautomatiseerde ondersteuning wordt besproken.

Inleiding

Menige organisatie heeft e-businessprojecten[1] geïnitieerd en/of gerealiseerd om de geïdentificeerde nieuwe commerciële mogelijkheden te benutten en/of de efficiëntie van de organisatie te verhogen. Inmiddels is gebleken dat e-businessinitiatieven ook nieuwe strategische risico's kunnen introduceren die het risicoprofiel en de waardering van de organisatie zowel in positieve als in negatieve zin kunnen beïnvloeden.

Dit artikel bespreekt een benaderingswijze voor het beheersen van risico's die ontstaan en/of significant veranderen als gevolg van e-businessinitiatieven in de organisatie of haar omgeving. Hierbij wordt ook ingegaan op het gebruik van ondersteunende hulpmiddelen bij het beheersen van dergelijke risico's. Een interessante praktijkcasus bij British Petroleum sluit het artikel af.

1) E-business wordt veelal aangeduid als het geheel van zakelijke handelingen die op elektronische wijze worden uitgevoerd ter verbetering van de efficiëntie en effectiviteit van de bedrijfsprocessen in een organisatie, gebruikmakend van internettechnologieën.

Impact e-business op organisaties

Afhankelijk van de sector waarin een bedrijf actief is, heeft de invoering van e-business meer of minder gevolgen voor de organisatie en haar processen. Met name de informatie-intensieve sectoren kwamen als eerste in aanraking met e-businessveranderingen. Voorbeelden van informatie-intensieve sectoren zijn de financiële dienstverlening, de overheid, de media- en uitgeverijsectoren, en de handel en distributie.

Figuur 1. Waardeketen (gebaseerd op het Porter-model).

E-businessinitiatieven initiëren c.q. versterken onder andere de volgende ontwikkelingen:

* *Het benutten van nieuwe marketing- en distributiekanalen*
De afstemming en integratie van de bestaande kanalen met het internetkanaal qua productaanbod, prijsbeleid en dienst/supportverlening teneinde de afzet en rentabiliteit van de bedrijfsactiviteiten te vergroten, vormen hierbij een uitdaging.

* *Het optreden van verschuivingen in de waardeketen*
Door uitbesteding en/of het overnemen van functies in de waardeketen is verdere efficiëntieverbetering te realiseren. Partijen nemen in de gewijzigde situatie meer of minder van de activiteiten in de keten voor hun rekening, en de onderlinge synchronisatie van processtappen tussen partijen is daarbij van groot belang.

* *De toename van prijstransparantie*
De e-businessontwikkelingen dragen samen met de introductie van de euro bij aan de (internationale) vergelijkbaarheid van productprijzen. Dit versterkt de noodzaak tot een concurrerend prijsbeleid en/of onderscheidende aspecten aan de producten en diensten.

* *Het toevoegen van een omvangrijkere informatiecomponent aan producten en diensten*
De toegevoegde informatiecomponent is vaak meer gericht op het vergroten van de klantenbinding dan op het realiseren van hogere marges op de producten.

* *Het vergroten van toegankelijkheid van informatie en systemen*
Door onder andere een e-procurementsysteem voor interne inkopen worden systemen meer en meer ontsloten voor grotere groepen medewerkers. Hierbij neemt de noodzaak toe tot formalisatie van inkoopprocedures en procuratieregels, zodat door de geautomatiseerde informatiesystemen onrechtmatige inkopen worden voorkomen.

* *Het intensiveren van interactie met medewerkers, partners, leveranciers en klanten*
De e-businessontwikkelingen maken het mede mogelijk de klantbehoeften systematisch in kaart te brengen en de marketing- en verkoopaanpak hierop af te stemmen. Het wordt onder andere mogelijk zeer gericht op geïdentificeerde behoeften en/of interesses marketingacties te initiëren zonder inbreuk te plegen op de privacy.

De e-businessontwikkelingen introduceren nieuwe kansen maar ook nieuwe c.q. gewijzigde (strategische) risico's die door een organisatie moeten worden gemanaged. Dit zogenaamde risicomanagement wordt hieronder uiteengezet.

Risicomanagement en e-business

Risicomanagement is een wat 'modieuze' benaming en een verbijzondering van een activiteit die feitelijk tot het normale management van organisaties behoort.

Een *risico* is de gemiddelde schade over een gegeven tijdsperiode, die verwacht wordt doordat één of meer bedreigingen leiden tot een verstoring van één of meer objecten van de informatievoorziening ([Over00]). En als men zich er wel van bewust is, worden de risico's niet altijd volledig en adequaat beheerst. Tegenwoordig komt steeds vaker in beeld dat websites gekraakt worden en dat elektronisch betalen niet altijd veilig is. Dit komt voor een deel doordat de gebruikte technologie in combinatie met de organisatorische aspecten ontoereikend functioneert.

Het management van een organisatie bepaalt of en zo ja, welke e-businessactiviteiten binnen de organisatie zullen worden gefinancierd. Maar het management is zich niet altijd bewust van de specifieke e-businessrisico's. Het komt vaak voor dat een organisatie pas maatregelen gaat nemen als er een incident is opgetreden. Er worden dan ad-hocmaatregelen getroffen voor dat specifieke incident, terwijl er beter naar een structurele oplossing gezocht kan worden. Deze gestructureerde oplossing kan door het risicomanagement worden aangeboden.

Risicomanagement omvat het op alle niveaus in de organisatie systematisch aandacht besteden aan het identificeren van onaanvaardbare kansen op marktverlies, imagoverlies, financiële verliezen, etc. Tevens worden in het kader van risicomanagement op een doeltreffende en economisch verantwoorde wijze maatregelen getroffen om de gevolgen van mogelijk te lopen risico's tot een aanvaardbaar niveau te reduceren, zodat een organisatie haar strategische doelstellingen kan blijven verwezenlijken.

Organisaties onderkennen meer en meer dat e-businessinitiatieven ook het risicoprofiel en de waardering van de organisatie in zowel positieve als negatieve zin kunnen beïnvloeden.

Een specifiek aandachtspunt hierbij vormt het beheersen van e-businessprojecten. De e-businessprojecten worden vaak gekenmerkt door een hoog inherent risicoprofiel. Vaak zijn het omvangrijke projecten die onder tijdsdruk via een prototyping- of Rapid Application Development-methode met onbeproefde en onvolwassen technologieën worden ontwikkeld. Andere factoren die bijdragen aan het hoge risicoprofiel zijn het grote aantal betrokken in/externe partijen, het ontbreken van expliciet gespecificeerde functionaliteiten en acceptatiecriteria, en het beperkte aantal interne medewerkers dat deel uitmaakt van de gebruikersgroepen.

Zowel het projectmanagement als auditors blijken vaak beperkte ervaring te hebben met het beheersen van de specifieke risico's die zich voordoen bij e-businessprojecten. Het gevolg hiervan is dat een groot aantal van deze projecten niet succesvol blijkt te zijn.

Gartner heeft vastgesteld dat 75 procent van de e-businessprojecten niet het vereiste eindresultaat oplevert.

Organisaties vertrouwen in de praktijk nog vaak op de deskundigheid van de medewerkers in de projecten als het gaat om het beheersen van e-businessrisico's. De projectmedewerkers zijn vaak beperkt in staat de consequenties van de e-businessinitiatieven te overzien. Met name risico's op gebieden die in mindere mate direct samenhangen met de ICT-projecten, zoals risico's op het gebied van branding, imago, beveiliging en het juridisch en fiscale gebied, worden vaak beperkt gemanaged.

Enerzijds ontstaan risico's doordat er een kloof ontstaat tussen de in de projecten impliciet aangenomen bedrijfseisen en de verwachtingen die bij het management leven, bijvoorbeeld over de geleverde functionaliteit van een webapplicatie in de beschikbare tijdsspanne. Anderzijds blijken talrijke activiteiten buiten de ICT-projecten te moeten plaatsvinden die niet door het e-businessproject kunnen worden beïnvloed, bijvoorbeeld de logistieke afhandeling van on line bestellingen van consumenten.

Organisaties die systematisch en planmatig aandacht besteden aan het beheersen van e-businessrisico's, geven dit vaak vorm door middel van een risicoanalyse en compenserende maatregelen vooraf en audits achteraf. In deze audits worden echter veelal niet alle relevante risicocategorieën betrokken.

De hierna geschetste aanpak voor risicomanagement in een e-businessomgeving beoogt het beheersen van e-businessrisico's deel te laten uitmaken van het normale management van de organisatie en de projecten. In de aanpak wordt expliciet aandacht besteed aan de mate waarin vanuit het project c.q. de organisatie de risico's kunnen worden beïnvloed. Alvorens de aanpak en gebruikte hulpmiddelen te behandelen, wordt eerst kort ingegaan op een aantal risico's die veranderen in een e-businessomgeving.

E-businessrisico's

Mede geïnitieerd door de e-businessontwikkelingen veranderen sommige condities waardoor bestaande risico's qua aard en invloed zich wijzigen en enkele nieuwe risico's voor organisaties worden geïntroduceerd. Onder meer de volgende veranderende condities beïnvloeden de risico's qua aard en omvang in een e-businessomgeving:

* De mogelijkheid om via internet een wereldwijde markt te bereiken en eventueel te bedienen leidt tot het ontstaan van culturele, politieke, fiscale en logistieke vraagstukken.
* Nieuwe concurrenten kunnen in bepaalde segmenten eenvoudiger toetreden; een website en een reclamebudget kunnen in principe toereikend zijn.
* De introductie van nieuwe businessmodellen, zoals on line informatiemakelaars en marktplaatsen, maar met ontbrekende ervaringsgegevens inzake 'best practices' en daadwerkelijke rendementen.
* De verkorting van de time-to-market en de snelle technologische veranderingen die de economische levens-

duur van producten beïnvloeden, met dito verkorting van afschrijvingstermijnen van e-businessinvesteringen. Dit maakt het ook weinig realistisch alle e-businessactiviteiten te plannen met een – binnen de organisatie gebruikelijke – tijdshorizon van drie à vier jaar.

* De veranderende rollen en relaties tussen bestaande partijen als leveranciers, afnemers, concurrenten en businesspartners. In sommige situaties zal met leveranciers en met name met concurrenten moeten worden samengewerkt om tot een volwaardige e-procurementmarktplaats in een bepaalde sector te komen.
* De verbondenheid met derde partijen, zoals Internet Service Providers, Application Service Providers, applicatieontwikkelaars, fulfilment bedrijven, telecommunicatiebedrijven, e-alliantiepartners, contentleveranciers, etc.
* De toegenomen afhankelijkheid van de ICT-infrastructuur en de daarmee samenhangende behoefte aan beschikbaarheid, schaalbaarheid en beveiliging van de informatiesystemen en bereikbaarheid van de helpdesk (bijvoorbeeld '365 × 24'-eis). Deze afhankelijkheid strekt zich uit tot systemen die zich buiten de beïnvloedingssfeer van de organisatie bevinden, zoals de pc's, palmcomputers en WAP-telefoons van gebruikers.
* De mogelijkheid tot reductie van menselijke interventie bij interorganisatorische processen en de daarmee samenhangende efficiëntievoordelen, met een sterk accent op standaardisatie van gegevensstructuren en processtappen.
* Het multidisciplinaire karakter van e-businesstoepassingen, waarin medewerkers met een bedrijfseconomische, juridische, verkoop-, marketing-, ICT-, logistieke en auditingachtergrond in 'begrijpelijke taal' moeten communiceren en samenwerken.
* De onzekere en complexe juridische en fiscale regelgeving, zoals BTW-heffing bij grensoverschrijdende transacties, jurisdictiekeuze en privacywetgeving.

In de hierna te behandelen aanpak met bijbehorende toolkit worden veranderende risico's in kaart gebracht voor de aandachtsgebieden zoals vermeld in figuur 2.

Figuur 2. Overzicht van aandachtsgebieden inzake veranderende risico's in een e-businessomgeving.

De veranderende risico's als gevolg van e-businessontwikkelingen worden hierna toegelicht. Deze verhandeling is zeker niet uitputtend, maar omvat een aantal voorbeelden van in de praktijk gesignaleerde risico's.

Bedrijfsprocessen

De e-businessontwikkelingen kunnen resulteren in een maximale bijdrage aan het resultaat van de organisatie indien de e-businessactiviteiten optimaal zijn afgestemd en geïntegreerd met de bestaande distributiekanalen en bedrijfsprocessen. Vaak blijkt dat er een discontinuïteit is tussen de reguliere processen en de aan de webomgeving gerelateerde processen, met bijvoorbeeld negatieve gevolgen voor de levering en facturering van orders. Tevens vinden er veranderingen en verschuivingen plaats in de wijze van klantbediening (bijvoorbeeld door on line productconfiguratie) en de wijze van opereren (bijvoorbeeld door het niet langer handmatig opstellen van offertes). Ook vindt er veelal beperkte integratie of afstemming plaats tussen de verschillende kanalen, zodat bijvoorbeeld de afhandeling van klantvragen en -klachten via e-mail of de afhandeling van retouren met grote vertraging of niet geschiedt.

Te vroege publicatie
Door een gebrek aan coördinatie zijn bij Austrian Airlines de financiële resultaten over het boekjaar 2000 vroegtijdig op het internet gepubliceerd. De directie heeft daarom direct de jaarcijfers officieel bekend moeten maken.

Achtergelaten e-winkelwagentjes
Uit onderzoek van BizRate.com en the NPD Group is gebleken dat circa 75 procent van de winkelwagentjes op websites wordt achtergelaten zonder dat het tot een aankoop is gekomen. Naast het niet kunnen vinden van het juiste artikel waren andere redenen hiervoor de hoge verzendkosten, de slechte performance en twijfels over beveiliging en privacy.

Geen kerstcadeau
Op de website van Toys 'R Us zijn een dag te lang bestellingen geaccepteerd. Gevolg was dat duizenden Amerikaanse gezinnen hun kerstcadeau pas na de Kerst ontvingen - met alle negatieve PR als consequentie. Er is zelfs een rechtszaak gevolgd vanwege het feit dat het bedrijf in zijn on line uitingen had aangegeven dat de bestellingen voor de Kerst zouden worden bezorgd.

Beveiliging

Het gebruik van het internet opent het eigen netwerk en de daaraan gekoppelde informatiesystemen voor een groot aantal potentiële gebruikers waaronder zich gebruikers bevinden die frauduleuze activiteiten niet schuwen (zie ook [KPMG01]). Het vaststellen van de identiteit van de gebruiker of partij die een on line transactie aangaat, is essentieel; hiervoor zijn technieken als digitale certificaten en handtekeningen te benutten. Daarnaast hebben bekende organisaties veelal hinder en imagoschade door interne fraude en hackingincidenten.

Creditcard lenen
Zowel Engelse als Nederlandse jongeren hebben tienduizenden creditcardnummers van websites weten te achterhalen. Dit gebeurde bij Amerikaanse, Canadese, Engelse en Japanse websites. Hiermee is intussen ook voor miljoenen guldens fraude gepleegd.
Reeds in 1998 bleek uit een onderzoek van Unterberg Towbin dat vijftig procent van de potentieel fraudeleuze VISA-transacties een internetoorsprong had, terwijl deze transacties slechts twee procent van het totaal uitmaakten.

Namaakbanken
De Amerikaanse Office of the Comptroller of the Currency heeft gewaarschuwd voor het bestaan van namaakwebsites van bekende banken. Websites met een licht afwijkende URL (webadres) maar met identieke 'look & feel' kunnen klanten in de val lokken om hun rekeningnummer en wachtwoord op deze illegale website in te voeren.

Fraude
Microsoft heeft verklaard dat haar Expedia-reissite per kwartaal een omzetderving van 4 tot 6 miljoen dollar heeft als gevolg van valse identiteitsgegevens.

Technologie

Veel webapplicaties zijn opgebouwd uit meerdere componenten aangezien weinig standaardproducten alle gewenste functionaliteit kunnen bieden, inclusief koppelingen met back-office systemen. Het toepassen van – frequent van versie veranderende – producten gecombineerd met maatwerk en 'middleware' resulteert door het ontbreken van een goede architectuur en gedegen testaanpak dikwijls in instabiele websites. Tevens kan een organisatie door de op de technologische ontwikkelingen naijlende standaardisatie 'op het verkeerde paard wedden' met het risico van kostbare infrastructurele aanpassingen en opleidingen later. Kritische technologische aspecten betreffen de beschikbaarheid, performance, schaalbaarheid en flexibiliteit van de systemen.

Storing
Uit onderzoek van de Boston Consulting Group is gebleken dat dertig procent van de websites te maken heeft met softwarestoringen die leiden tot beschikbaarheidsproblemen.

Wet- en regelgeving

Veranderingen in wetgeving c.q. rechterlijke uitspraken kunnen resulteren in een inconsistente regelgeving. Het is derhalve van belang dat de organisaties de zich snel wijzigende juridische kaders blijven volgen en indien mogelijk hier bij de ontwikkeling van webapplicaties en ICT-infrastructuren reeds op anticiperen. Voorbeelden van recente wetswijzigingen in Europa of in Nederland betreffen privacy, kopen op afstand, intellectuele eigendomsrechten en digitale handtekeningen. Ook onderwerpen als elektronische contracten, 'spam' (ongevraagde e-mail) en on line geschillenbeslechting worden momenteel in Europees verband besproken.

Nazi-artikelen
Een Parijse rechter heeft geoordeeld dat Yahoo niet langer nazi-artikelen via haar website mag aanbieden aan Franse burgers. Dit heeft Yahoo voor lastige technische uitdagingen gesteld en kan leiden tot precedentwerking in andere landen.

Marketinginformatie
Banken als US Bancorp, Bank of America en enkele andere zijn in de Verenigde Staten beschuldigd van de illegale verkoop van klantgegevens voor marketingdoeleinden. US Bancorp heeft voor een bedrag van enkele miljoenen dollars een schikking getroffen.

Branding

De reputatie en de 'goodwill' van een merk moeten ook in een e-businessomgeving worden bewaakt. Indien een organisatie in een on line omgeving onvoldoende beschermingsmaatregelen treft kan relatief eenvoudig reputatieschade worden aangericht of ongeautoriseerd misbruik worden gemaakt van het vertrouwen dat een merk bij een gebruiker heeft.

25 procent prijsverhoging
Onbekenden hebben kans gezien 25.000 vaste klanten van de Britse supermarktketen Safeway een met Safeway ondertekende valse e-mail te sturen. In deze e-mail werd aangegeven dat de prijzen met 25 procent werden verhoogd en dat de boodschappen beter bij de concurrentie konden worden aangeschaft.

007 onaantastbaar?
Vertrouwelijke financiële gegevens van klanten van Credit Suisse's internetbank, Direct Net, waren door fouten een week lang vrij toegankelijk over het internet. Klanten als Roger Moore, Udo Jürgens en andere prominenten overwegen stappen en verscheidene klanten hebben hun rekening inmiddels opgezegd.

E-businessrisicomanagementaanpak

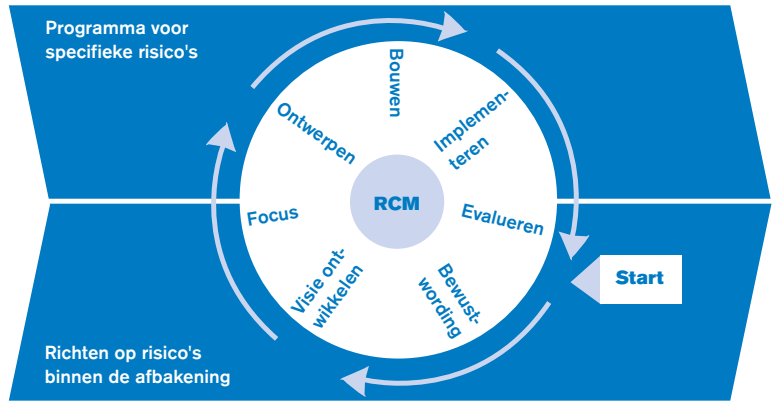
E-businesssponsors en -projectmanagers zijn zich vaak niet voldoende bewust van bovengenoemde risico's of hebben beperkte ervaring met het managen van deze risico's. Vaak ontbreekt daarnaast een centraal inzicht in de e-businessinitiatieven en de daarmee samenhangende risico's in organisaties.

De hierna toegelichte aanpak draagt zorg voor een toename van het bewustzijn van de nieuwe en gewijzigde risico's bij het reguliere management. Hiermee wordt beoogd het e-businessrisicomanagement deel te laten uitmaken van het normale management. Waardoor het risicomanagement bij e-businessinitiatieven in de organisatie of haar omgeving weer een proactief en preventief

karakter kan krijgen in plaats van een repressief karakter met ad-hoctegenmaatregelen na incidenten en audits achteraf.

Een gedegen risicomanagementaanpak helpt organisaties bij het op een consistente manier:
* verhogen van het bewustzijn bij het management rondom nieuwe en gewijzigde risico's door e-businessinitiatieven in de organisatie en/of haar omgeving. Het leereffect bij nieuwe e-businessprojecten door kennis te nemen van eerder ervaren risico's en gehanteerde oplossingen is een belangrijk onderdeel van risicomanagement;
* identificeren van relevante e-businessrisico's voor de organisatie;
* in kaart brengen van de getroffen maatregelen ter reductie van de kans dat de geïdentificeerde risico's zich manifesteren;
* ontwikkelen van een coherent actieplan om significante e-businessrisico's verder te reduceren en te beheersen.

Deze aanpak gaat uit van de in figuur 3 weergegeven managementcyclus.



Figuur 3.
Risk Control Method.

Bij KPMG Information Risk Management is de Risk Control Method (RCM) ontwikkeld. Dit is een methode voor het risicomanagement om in een organisatie op gestructureerde wijze de risico's te kunnen beheersen.

De Risk Control Method bestaat uit de volgende stappen:
1. *Bewustwording.* Tijdens deze stap krijgen het management en de medewerkers inzicht in de risico's en worden ze op de hoogte gebracht van de noodzaak van maatregelen tegen de risico's.
2. *Visie ontwikkelen.* Tijdens deze stap wordt de IST-situatie beschreven, het beleid opgesteld en een risicoanalyse of afhankelijkheids- en kwetsbaarheidsanalyse uitgevoerd.
3. *Focus.* Tijdens deze stap worden uit het verkregen inzicht van de IST-situatie, de SOLL-situatie en een beveiligingsplan opgesteld.
4. *Ontwerpen en bouwen.* Tijdens deze stap worden de maatregelen ontworpen en gebouwd.
5. *Implementeren.* Tijdens deze stap worden de ontworpen en gebouwde maatregelen daadwerkelijk geïmplementeerd.
6. *Evalueren.* Tijdens deze stap worden de maatregelen gecontroleerd, beheerd en continu verbeterd.

Ook door diverse andere auteurs en organisaties zijn risicomanagementaanpakken ontwikkeld, zoals door het NGI ([NGI92]) en Cox en Tait ([Cox91]).

Hoewel de aanpak ook zonder geautomatiseerde hulpmiddelen goed kan worden toegepast, biedt een geautomatiseerd hulpmiddel als de hier beschreven 'e-business risk planning toolkit' een aantal voordelen, te weten:
* Het is eenvoudiger om kennis en ervaring te bundelen en gestructureerd te ontsluiten voor het (midden)-management.
* Het lokale management kan op een efficiënte manier zelf de relevante risico's voor het betreffende organisatieonderdeel identificeren en hierover op een consistente en vergelijkbare manier rapporteren. Dit geldt evenzo voor de actieplannen en beheersingsmaatregelen.
* Op centraal niveau kan het senior management inzicht houden in de e-businessinitiatieven en de daarmee samenhangende specifieke risico's.
* De aanpak kan eenvoudiger op een consistente wijze in de organisatie worden ingevoerd.

De RCM-aanpak is dan ook geïmplementeerd in de 'e-business risk planning toolkit'. In figuur 4 zijn op hoofdlijnen de belangrijkste componenten van deze toolkit weergegeven.

De aanpak bestaat uit de volgende activiteiten:

* *Kick-off*

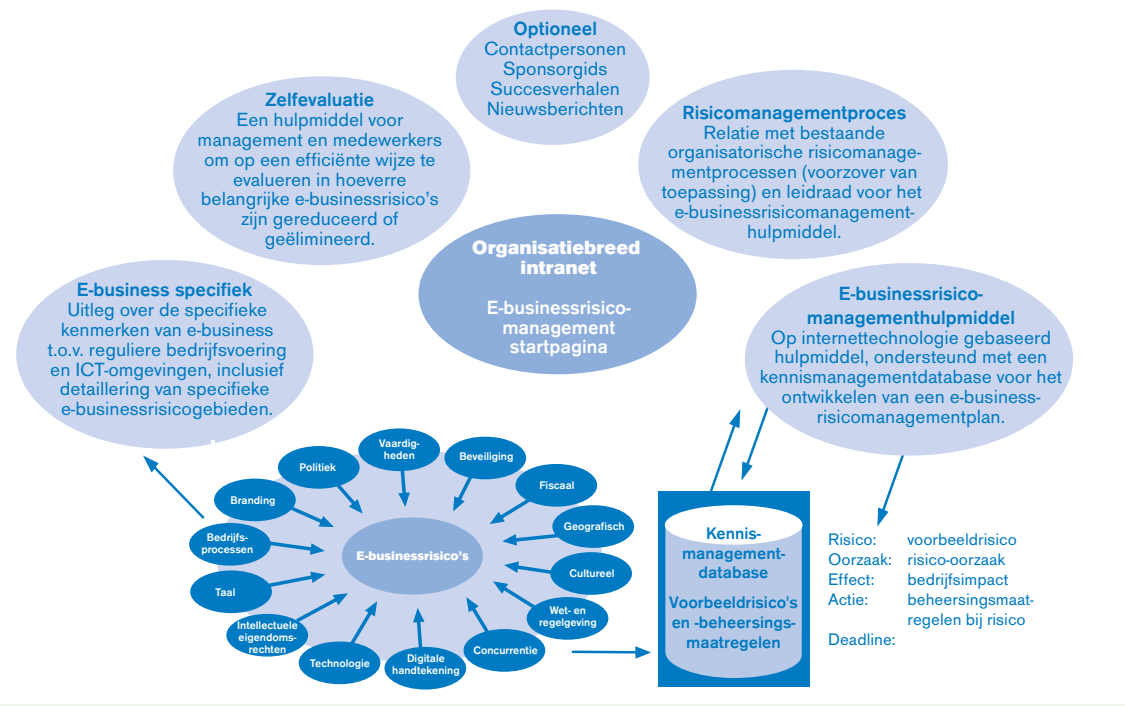
In een workshop worden de scope en de planning van het risicomanagementproject nader toegelicht en volgens een contingentiebenadering verder toegespitst op de concrete organisatiesituatie. Bij deze workshop worden de verantwoordelijken c.q. sponsors ten aanzien van e-business uit de diverse organisatieonderdelen betrokken. Eventueel kunnen zelfs externe 'stakeholders' erbij betrokken zijn, zoals in het geval van een on line marktplaats of een e-businessproject in de keten (bijvoorbeeld bij een supply chain management-project).

* *Risicobewustzijnssessie*

In kaart wordt gebracht welke veranderingen in de risico's door de e-businessinitiatieven zich zullen voordoen en/of zich hebben voorgedaan. Op grond van deze basisinventarisatie wordt in kaart gebracht welke risico's in de specifieke situatie in de betreffende organisatie met name zijn gewijzigd en wordt de zelfevaluatievragenlijst aangepast aan de specifieke organisatiesituatie. In een workshop met de sponsors wordt geverifieerd of de juiste (aansprekende) risico's zijn geselecteerd voor de bewustzijnssessies bij de diverse organisatieonderdelen.

* *Integreren e-businessrisicomanagement in de reguliere management control*

Het is van belang e-businessrisicomanagement te verankeren in de reguliere risicomanagementprocessen. In deze fase wordt geïnventariseerd welke risicomanagementprocessen operationeel zijn en hoe e-businessrisico-



Figuur 4. Risicomanagement-processen en -systemen.

management in de reguliere risicomanagementprocessen kan worden geïntegreerd. Het uiteindelijke doel is e-businessrisicomanagement weer deel te laten uitmaken van het normale managementinstrumentarium en er geen verbijzonderde activiteit van te maken.

* *Toespitsen kennisdatabase op de specifieke situatie*

De relationele kennisdatabase bevat alle geïdentificeerde risico's, oorzaken, organisatiegevolgen en beheersingsmaatregelen in een gestructureerde vorm. Het is van essentieel belang dat de kennisdatabase wordt toegespitst op de specifieke situatie waarin het hulpmiddel wordt ingezet. Dit betekent enerzijds dat terminologie wordt aangepast aan de omgeving waarin de organisatie opereert en anderzijds dat wordt geëvalueerd op welke punten de standaardset met risico's en beheersingsmaatregelen niet representatief is. Dit betekent dat op onderdelen in het voortraject reeds risico's en maatregelen worden geschrapt en/of toegevoegd.

* *Validatie kennisdatabase door het management*

De aangepaste set met e-businessrisico's en maatregelen wordt gevalideerd door vertegenwoordigers van het management. Dit draagt ertoe bij dat het management in een vroegtijdig stadium wordt betrokken in het traject voor het creëren van bewustzijn (en het vrijmaken van het benodigde budget).

* *Pilotimplementatie e-businessrisicomanagement*

In een pilot worden alle fasen (Identificeer, Evalueer, Actie) uit de e-businessrisicomanagementaanpak doorlopen. Op basis van de ervaringen wordt de aanpak geëvalueerd en waar nodig bijgesteld en vervolgens uitgerold in de organisatie.

* *Uitrol e-businessrisicomanagement bij de organisatieonderdelen*

De invoeringsvolgorde qua organisatieonderdelen kan worden bepaald aan de hand van criteria als de hoogte van de e-businessinvestering, de omvang van de on line transacties en het risicoprofiel van de e-businessactiviteiten. De verdere invoering van deze aanpak wordt vergemakkelijkt door het 'rijker' worden van de kennisdatabase.

E-businessrisicomanagementhulpmiddel

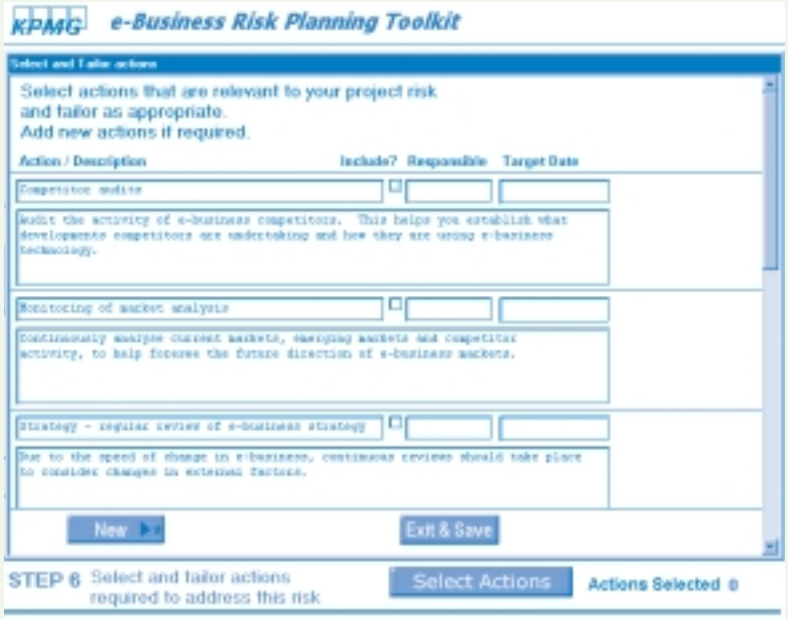
In deze paragraaf wordt nader toegelicht op welke wijze het e-businessrisicomanagementproces in een aantal concrete stappen is vormgegeven in de 'e-business risk planning toolkit'.

Van belang is dat de manager op basis van een aantal criteria kan vaststellen welke e-businessrisico's voor hem of haar relevant zijn. In figuur 5 zijn de geïdentificeerde variabelen weergegeven die het een manager mogelijk maken de voor hem/haar relevante risico's te selecteren.

Door het invoeren van een viertal onderscheidende criteria kan een manager de relevante e-businessrisico's selecteren uit de totale set met e-businessrisico's. De selectiecriteria betreffen:

Figuur 5. Identificeren van relevante risico's.

Figuur 6.
Criteria voor risicoselectie.



Figuur 7.
Keuze van beheersingsmaatregelen.

* *Business stage*. De business stage geeft de fase aan waarin het e-businessinitiatief zich bevindt, van strategische voorbereiding, implementatie tot de operationele beheersituatie.
* *Geo-political areas.* Hiermee wordt het continent of de regio aangeduid waar het zwaartepunt van de activiteiten zal liggen. Met name op het gebied van wet- en regelgeving, cultuur en markt kunnen de omstandigheden aanzienlijk verschillen.
* *Business objectives.* De na te streven doelstelling voor e-businesstoepassing kan hiermee worden gekarakteriseerd, van eenvoudige informatie-uitwisseling tot en met de integratie van e-business met de back-office systemen.
* *Issues.* De aspecten die relevant zijn voor het betreffende initiatief of project, van juridische en fiscale tot aan strategische en beveiligingsrisico's.

Op deze wijze worden die e-businessrisico's geselecteerd die ontstaan c.q. veranderen als gevolg van e-businessontwikkelingen in een organisatie en/of haar omgeving (zie figuur 6).

Op basis van de ingevoerde selectiecriteria worden in het voorbeeld van figuur 6 door de e-business Risk Management-applicatie voor de fase Strategie acht risico's onderkend voor het issue Concurrentie. Eén van de onderkende risico's betreft de situatie waarin een concurrent eerder een bepaalde e-businessoplossing aanbiedt in deze markt. Voor ieder van de onderkende issues dient de manager vast te stellen wat de impact en beheersbaarheid van de aangepaste e-businessrisico's in zijn specifieke situatie zijn (stap 5). Vervolgens dient een inschatting te worden gemaakt van de kans van optreden en de impact van het risico op de bedrijfsvoering. Tevens dient hierbij te worden vastgesteld in welke mate het onderkende risico kan worden beheerst door de organisatie. Hierbij wordt onderscheid gemaakt tussen risico's die men wel en die men niet kan beïnvloeden.

Op het moment dat is vastgesteld of een risico relevant is en derhalve wordt opgenomen in het risicomanagementplan, kan worden vastgesteld welke acties gewenst zijn om de e-businessrisico's te beheersen. De kennisdatabase biedt de manager al een handreiking met relevante te treffen maatregelen waarvan men kan besluiten ze al dan niet op te nemen in het risicomanagementplan (zie figuur 7). Hierbij bestaat de mogelijkheid de formulering van de actie verder toe te spitsen op de specifieke situatie en/of aanvullende maatregelen toe te voegen aan de kennisdatabase.

Op basis van de doorlopen stappen in het e-businessrisicomanagementproces ontstaat uiteindelijk een samenhangende en consistente set met risicomanagementplannen. Deze benaderingswijze draagt ertoe bij dat risicomanagement een meer proactief karakter krijgt. Immers, de e-businessrisico's worden niet alleen tot een minimum beperkt maar ook kansen worden eerder maximaal benut doordat projectrisico's beter worden beheerst en er eerder wordt geanticipeerd op bedreigingen.

Praktijkcasus

De hiervoor beschreven methode en toolkit voor het beheersen van e-businessrisico's zijn bij British Petroleum (hierna BP) met succes in de praktijk toegepast. In deze paragraaf wordt beschreven:

* waarom BP specifiek aandacht wenste te besteden aan e-businessrisicomanagement;
* hoe het beheersingsraamwerk en de kennisdatabase tot stand zijn gekomen;
* welke voordelen de aanpak heeft geboden voor BP.

Waarom aandacht voor e-businessrisicomanagement binnen BP

BP's visie om tot een digitale onderneming te evolueren heeft geleid tot een groot aantal e-businessinitiatieven. De initiatieven varieerden sterk in aard en omvang. Enerzijds was er een groep projecten die zich richtte op interne efficiëntie zoals e-procurement (on line inkoop) en e-HR (on line personeelszaken met mogelijkheden tot het à la carte selecteren van arbeidsvoorwaarden). Anderzijds waren er onder meer projecten gedefinieerd die zich richtten op het verbeteren van de dienstverlening aan klanten en het daarbij gelijktijdig reduceren van de kosten. Tot slot waren projecten gedefinieerd die zich richtten op het ontwikkelen van nieuwe producten en klantapplicaties.

Duidelijk was dat BP door de e-businessinitiatieven talloze nieuwe kansen zou kunnen benutten. In een vroegtijdig stadium werd echter ook gesignaleerd dat door de e-businessinitiatieven het risicoprofiel van de onderneming kon worden beïnvloed. BP onderkende dat het beheersen van deze nieuwe risico's essentieel was voor de onderneming en besloot tot het ontwikkelen van een aanvullend beheersingsraamwerk. Dit beheersingsraamwerk had tot doel de nieuwe e-businessrisico's tot een minimum te beperken terwijl daarbij toch maximaal de kansen kunnen worden benut die de e-businessinitiatieven BP bieden.

Het e-businessbeheersingsraamwerk had tot doel:
* het management van BP te helpen bij het identificeren, beoordelen en communiceren van de e-businessrisico's; hierbij was het mogelijk een zelfevaluatie uit te voeren;
* het voorzien in richtlijnen en een plan van aanpak waaruit blijkt welke beheersingsmaatregelen noodzakelijk zijn om de geïdentificeerde beheersingsmaatregelen tot een qua aantal acceptabel niveau terug te brengen.

De totstandkoming van het BP e-business-beheersingsraamwerk en de BP-kennisdatabase

Ten behoeve van BP is een specifiek BP e-businessbeheersingsraamwerk ontwikkeld en is tevens een specifieke kennisdatabase ontwikkeld met voorbeelden van risico's en hieraan gerelateerde beheersingsmaatregelen. Het beheersingsraamwerk en de kennisdatabase zijn ontwikkeld op basis van uitgebreide research en het raadplegen van KPMG-experts.

De opzet voor het beheersingsraamwerk en de specifiek op de BP-situatie toegespitste kennisdatabase is gevalideerd en waar nodig aangevuld gedurende een tweedaagse workshop. Aan deze workshop hebben dertig BP-managers en e-champions uit Europa en Noord-Amerika deelgenomen.

In dit proces is vastgesteld dat voor de effectiviteit van e-businessrisicomanagement het in de praktijk van belang is dat:

* de focus wordt gelegd op risico's die zich specifiek manifesteren c.q. zich significant wijzigen in een e-businessomgeving;
* onderscheid wordt gemaakt naar de fase waarin de e-businessinitiatieven zich bevinden. Inmiddels wordt expliciet onderscheid gemaakt in risico's en beheersingsmaatregelen die relevant zijn voor de fasen Strategie, Implementatie en Operatie.

Ervaren voordelen van de aanpak en toolkit voor BP

De volgende voordelen zijn onderkend door het toepassen van de beschreven aanpak en tooling voor het beheersen van e-businessrisico's:

* *Toegenomen bewustzijn bij het management inzake e-businessrisico's*
De hulpmiddelen en het trainingsprogramma hebben ertoe bijgedragen dat risico's van e-businessinitiatieven tijdig worden onderkend opdat acties konden worden ondernomen om de onderkende risico's te reduceren tot een acceptabel niveau. Het aanmerken van lijnmanagers en e-businessprojectmanagers als belangrijkste gebruikers en gegevensverantwoordelijken heeft ervoor gezorgd dat het bewustzijn omtrent nieuwe en gewijzigde risico's bij hen snel steeg.

* *Versnelling van projectimplementaties*
De proactieve en consistente manier van het managen van e-businessrisico's droeg ertoe bij dat de eisen in een eerder stadium en explicieter in het project werden gedefinieerd, waardoor de projecten zich meer konden concentreren op het opleveren van de gewenste oplossingen.

* *Consistente aanpak e-businessrisicomanagement in de organisatie*
De gestandaardiseerde richtlijnen en (geautomatiseerde) hulpmiddelen waarborgden een consistente aanpak om e-businessrisico's te managen over de organisatieonderdelen heen.

* *Meer focus op de juiste e-businessrisico's*
De aanpak richt zich op het treffen van beheersingsmaatregelen ten aanzien van de geïdentificeerde hoge risico's, hetgeen waarborgt dat de inspanning voor het treffen van additionele maatregelen zich richt op die plaatsen waar de effectiviteit het hoogst is en dat de financiële middelen derhalve optimaal worden aangewend.

* *Beperkte implementatietijd e-businessrisicomanagement*
De methode en applicatie zijn ontwikkeld en geïmplementeerd in negentig dagen. Hierbij is er tevens voor gezorgd dat de applicatie is geïntegreerd met BP's intranet.

Het door organisaties zelf op een systematische manier identificeren en evalueren van e-businessrisico's heeft geleid tot een sterker risicobewustzijn en tot een flinke verbetering op het vlak van vroegtijdig identificeren en systematisch managen van geïdentificeerde risico's.

Drs. ing. R.F. Koorn CISA RE
is senior manager e-Business Services bij KPMG Information Risk Management te Amstelveen. Zijn specialisaties zijn e-business, Public Key Infrastructures, e-procurement en on line privacy. Hij is twee jaar voor KPMG werkzaam geweest in San Francisco en Silicon Valley.

Drs. B.H.M. Peters RA
is senior manager bij KPMG Information Risk Management te Arnhem. Zijn aandachtsterreinen zijn de assuranceaspecten van e-business, ICT-governance en informatiebeveiliging.

P. Freeborn MSc
is senior manager bij KPMG Information Risk Management te Londen. Hij is verantwoordelijk geweest voor de ontwikkeling van KPMG's methode en geautomatiseerde hulpmiddelen voor e-business-risicomanagement.

Conclusies

Door onvoldoende, te late of ongestructureerde aandacht en aanpak ondervinden vele organisaties e-businessrisico's aan den lijve. Uit onze praktijkervaring lijkt het of we de fouten uit de beginjaren van de automatisering aan het herhalen zijn nu het internet betreft. Ondanks het feit dat er al meerdere jaren ervaring is opgedaan met e-businessprojecten, blijkt dat door de toegenomen bedrijfseisen en onervaren projectmanagers de specifieke e-businessrisico's nog immer tot aanzienlijke problemen leiden.

Indien bij het toepassen van e-businessrisicomanagement een brede scope wordt gehanteerd, met naast de reguliere ICT-onderwerpen ook onder andere strategische, financiële, management-, logistieke en marketingaspecten, kan e-businessrisicomanagement een uiterst nuttige bijdrage leveren aan het succesvol maken van e-businessinitiatieven.

Nadat een organisatie allereerst expliciet de e-businessrisico's heeft geanalyseerd en zo nodig gereduceerd, kan deze separate exercitie vervolgens worden geïntegreerd in de reguliere risicomanagementaanpak. De opgedane kennis en ervaring door zelfevaluaties en gezamenlijke analyses en actieplanning dient hierbij wel beschikbaar te blijven voor nieuwe e-businessactiviteiten.

Kortom: goede e-business kan niet zonder risicomanagement!

Literatuur

[Cox91]
S.J. Cox en N.R.S. Tait, *Reliability, Safety & Risk Management; An Integrated Approach*, Butterworth-Heinemann, 1991.

[NGI92]
NGI, *Risicoanalyse en risicomanagement*, Kluwer Bedrijfswetenschappen, 1992.

[Over00]
P. Overbeek, E. Roos Lindgreen en M. Spruit, *Informatiebeveiliging onder controle*, Prentice Hall, 2000.

[KPMG01]
KPMG, Global e.fr@ud.survey, www.kpmg.nl/irm, 2001.