Risicobeheer en compliance als uitgangspunt

VISIO ON STEROIDS

Eerst alle processen in kaart brengen, vervolgens nagaan wat er binnen die processen eventueel fout kan gaan en alleen op die punten actie ondernemen. Dat is de kern van risicobeheer en procesmodellering, stelt Luc Brandts van BWise. De markt begint in te zien dat hier een platform voor nodig is. "We gaan gouden tijden tegemoet."

Door Teus Molenaar

Op de geologische schaal stelt het niets voor, relativeert Brandts, chief technology officer van Bwise, maar volgens IT-begrippen heeft het bedrijf al een lange historie achter de rug. Aanvankelijk is ingezet op het simuleren en modelleren van processen, maar tegenwoordig is het bedrijf gespecialiseerd in risicobeheer en compliance. In mei 2002 heeft het de modelleringsoftware SDW (System Development Workbench) overgenomen van Capgemini, voornamelijk vanwege het klantenbestand en het goede team. Brandts zegt het liefst voor de muziek uit te willen lopen. "Maar niet te ver, anders mis je het contact met de markt." Zo komt hij met het voorbeeld dat zijn bedrijf als eerste (in 1999) een dynamische webserver presenteerde. Dat betekent dat een gebruiker, wanneer hij inlogt, alleen die processen krijgt te zien die voor hem relevant zijn. Als hij wil, kan hij ook die duizend andere processen zien, terwijl bij andere tools de gebruiker meteen het complete processenpakket voor zijn kiezen krijgt.
In het jaar 2000 zag Brandts dat het gebruik van modellering- en simulatie-tools gemeengoed werd. "Daar viel eigenlijk geen onderscheid meer te maken. De ene tool heeft net een paar features meer dan de andere, maar dat zou een gebruiker nooit opvallen. We moesten een andere kant op."

Andere afslag

Dat is risicobeheer geworden. Dat sluit aan bij Brandts' idee dat je vanuit processen denkend een organisatie kunt optimaliseren. "Stel dat je binnen een organisatie ontdekt dat je zestien verschillende manieren hebt om jouw klanten te betalen. Je kunt dan die processen gaan automatiseren, maar het is natuurlijk veel logischer om dit proces te standaardiseren tot één manier van betalen, want dan hoef je maar één proces te automatiseren in plaats van zestien. Dat zal iedereen met je eens zijn. Maar je moet je ook afvragen waarom er zestien verschillende methoden zijn. Misschien wordt er gewerkt in zestien verschillende landen met elk hun eigen wetten en regels, of misschien heb je veertien verschillende systemen, of verschillende organisaties met hier honderd man en daar duizend mensen, of historische verschillen. Allerlei zaken die een dergelijke standaardisatie tot een waar avontuur maken."
Er zijn grofweg twee methodes om dit probleem aan te pakken, meent Brandts. De ene is het leveren van consulting: adviezen geven over zo'n standaardisatieslag. Daar hebben volgens hem de meeste concurrenten voor gekozen. "Alle concurrenten uit de jaren tachtig, negentig zie ik niet meer terug. Zij leveren ook wel tooling, maar die is vaak heel complex. Want waar heb je anders die consultants voor nodig?"

> **Negentig procent van de bedrijven behelpt zich met spreadsheets**

BWise heeft heel bewust een andere afslag genomen. "Wij zetten onze tooling in als een bedrijfsapplicatie. Dat betekent dat je gebieden moet vinden, als organisatie, waarop een proces heel dominant is om je daar vervolgens op te richten. Dat is voor ons risicobeheer geworden en het voldoen aan wetten en regels." De komst van de Wet Sarbanes-Oxley in mei 2002 heeft laten zien dat BWise op het juiste paard heeft gewed. Want GRC (Governance, Risk and Compliance) is 'hot'.

Forrester

Vaak wordt bij governance en compliance gedacht aan het grootboek; als dat maar op orde is, dan kunnen de auditeurs hun handtekeningen zetten. Maar een GRC-platform is veelomvattender. Om met Brandts te spreken: "Je moet

bijvoorbeeld kunnen aantonen dat de medicijnen die jij maakt voldoen aan de wettelijk gestelde eisen en dat de hoeveelheid van een bepaalde stof die ze bevatten niet dodelijk is. Niet alleen de bankwereld stelt eisen aan risicobeheer, maar de Food and Drug Administration (FDA) doet dat evenzeer. En zo zijn er tientallen instanties en honderdtallen regels."

Een GRC-platform bestrijkt, aldus Forrester Research, vier gebieden: beleid, procedures, controledocumentatie en communicatie; inschatting van risico's en controlemogelijkheden; risico-analyse; beheer van verlies, gebeurtenissen en onderzoek. Uit de jongste ForresterWave over GRC komen BWise en IBM als beste uit de bus. Helemaal bovenaan staan Axentis en Qumas, zij het dat deze zich op deelterreinen begeven. Qumas richt zich louter op financiële instellingen en 'life sciences', en Axentis alleen op software as a service. "Per 10 april hebben wij ook de SAS-70 type 11-certificatie van KPMG gekregen, zodat diegenen die onze oplossing als een hosted versie gebruiken, dat nu ook met een gerust hart kunnen doen", klinkt het trots uit Brandts' mond.

Volgens Brandts is de juiste volgorde om eerst na te gaan of een proces goed in de organisatie ligt. "Maar om het proces goed te begrijpen moet je weten wat er mis kan gaan; dat zijn de risico's. Vervolgens ga je voor die gevallen waar het vervelend is als er iets mis gaat beheermaatregelen treffen. Onze volgorde is: proces, risico, beheer."
BWise heeft sinds 2000 een vestiging in New York (en eentje in India voor het 'gewone' ontwikkelwerk). Toen SOX van kracht werd, is de Amerikaanse tak van het bedrijf benaderd door Ernst & Young om compliance-maatregelen goed op de rit te zetten. Eén van de adviseurs van BWise in New York heeft meegewerkt aan de COSO Guide for Small and Medium Companies dat vorig jaar is uitgegeven. Deze gids laat bedrijven uit het MKB-segment zien hoe ze kunnen voldoen aan de wet- en regelgeving zonder te kapseizen als gevolg van de dure consultancy- en auditing-kosten.

Foto: Harry Otto.

Dr.ir. Luc Brandts: "Bouw een schil rond alle processen".

Spreadsheets

Op de tegenwerping dat ook de grote ondernemingen steen en been klagen over de kosten die SOX en andere regelgevingen met zich meebrengen, stelt Brandts dat het eigenlijk wel meevalt, omdat negentig procent van die bedrijven zich behelpt met spreadsheets. Als grootste concurrent noemt hij dan ook zonder aarzelen: Excel van Microsoft. "De specifieke GRC-leveranciers, zoals wij, hebben hooguit vijf procent van de markt. De overige 95 procent doet het met Excel, Word en Visio. Maar het is onmogelijk om aan het eind van het jaar een helder inzicht te hebben in veertigduizend spreadsheets. Organisaties zijn wel bezig dit terug te brengen, maar dan heb je het soms nog over dertigduizend spreadsheets. Zelfs al zijn het er duizend, dan nog kun je daar eigenlijk niets mee. Uiteindelijk tekenen de cfo en auditor wel, maar dat is meer uit onmacht. Vandaar dat de grote bedrijven nu wel naar ons toekomen, want ze willen van die problemen af. Wat dat betreft is er wel een omslag gaande."
Vijf jaar geleden had Brandts nog Europese concurrenten, maar nu zijn dat allemaal Amerikaanse bedrijven. "De Europeanen zijn blijven hangen op het proces-stuk. Ze zijn veel te weinig aan het denken geweest in tools. Het is heel wat anders om een tool te bouwen dan een applicatie. De meeste tool-bouwers kunnen geen applicaties maken. Met een tool kun je van alles doen, het is vreselijk flexibel. Maar als je een specifiek probleem wil aanpakken, dan moet een tool met van alles en nog wat optuigen, waardoor het voor de business-gebruiker onbegrijpelijk wordt.
Aan de Amerikaanse kant van de markt zie je dat ze daar geweldig goed applicaties hebben gebouwd die controls

kunnen identificeren, beheermaatregelen kunnen identificeren en deze kunnen aftekenen. Ze zoeken er bewijsmateriaal bij en presenteren het geheel in een prachtig rapport. Het probleem bij deze benadering is dat het heel erg bottom-up is. Je hebt bij wijze van spreken veertigduizend controls. Dat zijn geen spreadsheets, maar punten in een applicatie waar iets fout kan gaan. De vraag is dan wat je met veertigduizend controls moet doen. Dat is net zo onoverzichtelijk.
Onze benadering is top-down: we beginnen met het proces en maken pas beheermaatregelen op plaatsen waar dat echt nodig is. De Amerikanen missen de proces-kant en de Europeanen de applicatie-aanpak. Wij zitten er tussenin, want we bieden beide."
De Amerikaanse leveranciers zien de pijnpunten in een proces en gebruiken vervolgens Visio om het proces te modelleren en zo de risico's te verminderen. "Aan het eind van het liedje zijn er heel veel Visio-diagrammen die geen enkel onderling verband hebben. Als iets in één proces wijzigt, dan moet je tientallen andere diagrammen ook handmatig door om na te gaan of die wijziging daar effect heeft. Bij ons is dat geïntegreerd. De Amerikanen noemen onze benadering ook wel 'Visio on steroids'."

Geen hype

Door de processen als uitgangspunt te nemen, en te modelleren waar nodig, krijg je de hoogst mogelijke managementaandacht, zo meent Brandts. "Wij zaten altijd wel met de controller rond de tafel, maar nu praten we met de cfo of de ceo. Het gaat echt lang duren, maar het hele gedoe rond compliance brengt Business Perfomance Management op de agenda. Dat is geen hype zoals business process redesign."

> De vraag is wat je met veertigduizend controls moet doen

Bij het management dringt het belang door dat het nodig is de risico's te beheren en waar nodig de processen aan te pakken. De markt van aanbieders om de bestuurders bij te staan is volop in beweging. Er is aan de ene kant consolidatie gaande waarbij bedrijven worden opgekocht, en aan de andere kant onderlinge samenwerking. Zo werkt BWise samen met Business Objects en heeft een OEM-overeenkomst voor de rapportage-tool van dit bedrijf. De Nederlanders hebben een eigen content management oplossing, maar werken ook samen met Filenet (onderdeel van IBM). Op zijn beurt is Cartesis overeengekomen om de GRC-suite van BWise te integreren in zijn performance management-oplossing. De inkt van de handtekeningen onder deze overeenkomst was nog niet droog of Business Objects meldt (op 23 april j.l.) Cartesis te hebben overgenomen. "Dit doet niets af aan de deal die wij met Cartesis hebben gemaakt", weet Brandts te vertellen. "Dat was ook wel te verwachten, want wij werken al nauw samen met BO."

Kruisverbanden

SAP is *big time* bezig de GRC-markt te betreden, zegt Brandts. De consolidatie is ingezet en er zullen kruisverbanden ontstaan. "Niemand kan dit alleen doen. Je moet blijven focussen op waar je goed in bent. Wij bouwen een schil rond alle processen in een bedrijf, maar SAP neemt de transacties als uitgangspunt. Dat snap ik wel, en als ik SAP was, zou ik het ook zo doen, dat bedrijf is immers 'eigenaar' van de transacties, maar dan ben je wel heel erg geïntegreerd met de processen in plaats van een schil erom heen."
Kruisverbanden ziet hij tussen GRC-leveranciers en makers van software voor ERP, BPM, integratie (zoals Cordys), en Corporate Performance Management (zoals Cartesis). Niet alleen vanwege functionaliteit, maar ook vanwege wereldwijde aanwezigheid.

Teus Molenaar is freelance journalist.

Werktuigbouwkundige

Je moet hem geen machines laten ontwerpen of bouwen, maar het proces om tot een goede machine te komen, is bij hem in goede handen. Luc Brandts heeft werktuigbouwkunde gestudeerd aan de TU Eindhoven, gespecialiseerd in simulatie en optimalisering. Hij is er gepromoveerd op het onderwerp 'ontwerpen van systemen/organisaties'. Na een aantal jaar te hebben gewerkt als consultant, belast met systeemimplementaties, change management en procesoptimalisering in de IT-sector, heeft hij samen met anderen het bedrijf BWise opgericht in 1994.