

# Enterprise Risk Awareness Integraal risicomanagement voor continuïteit en concurrentievoordeel

**Het is voor organisaties harde noodzaak om risico's voor de bedrijfsvoering effectief te beheersen. Helaas wordt risicomanagement in de praktijk nog te vaak geïsoleerd opgepakt. Hoe kan de manager deze isolatie doorbreken en hoe kan hij/zij risico's integraal beheersen? Enkele handvatten.**

Risicomanagement is de afgelopen jaren in de meeste organisaties gestegen naar de bovenste regionen van de managementagenda. De omgeving van organisaties verandert sterk, momenteel zorgt de kredietcrisis voor veel onzekerheid. De betrouwbaarheid van leveranciers verandert, financiering is moeilijker en klanten zijn terughoudender met investeringen. Organisaties willen financiële en imagoschade voorkomen en regelgevers eisen 'compliance', waarbij managers soms zelfs persoonlijk aansprakelijk worden gesteld voor het onvoldoende beheersen van risico's. Zo berichtte de *New York Times* onlangs dat zeker twaalf topmanagers van de omgevallen zakenbank Lehman Brothers zijn gedagvaard.

Organisaties beheersen hun bedrijfsrisico's in de praktijk vaak onvoldoende effectief en inefficiënt. De kern van het probleem is dat veel organisaties risico's binnen afzonderlijke functionele gebieden beheersen: het silodilemma. Het gevolg hiervan is dat een integraal beeld van de risicoblootstelling op organisatieniveau ontbreekt en de risicobeperkende maatregelen niet op elkaar worden afgestemd. Wij zijn van mening, dat organisaties op de langere termijn hun continuïteit kunnen waarborgen en zelfs concurrentievoordeel kunnen behalen door hun risico's beter te beheersen. Zelfs in deze onzekere tijd is Rabobank in staat nieuw geld aan te trekken, deels ten koste van haar concurrenten vanwege haar imago als één van werelds veiligste banken.

We beschrijven waarom risicomanagement de afgelopen periode is gestegen op de managementagenda en hoe risico's de huidige en toekomstige winstgevendheid van organisaties bedreigen. Een deel van deze bedreigingen komt voort uit het zogenaamde silodilemma. Integraal risicomanagement wordt als oplossing voor de gevolgen van het silodilemma gepresenteerd. Vervolgens krijgt de manager concrete handvatten om integraal risicomanagement binnen zijn/haar organisatie in te voeren. Deze handvatten stellen hem/haar in staat zijn/haar portfolio van risico's en maatregelen in samenhang te beheersen om daarmee continuïteit en concurrentievoordeel te creëren.

## **Risicomanagement stijgt op de managementagenda**

Klanten stellen steeds hogere eisen aan de kwaliteit van producten en diensten. Waar bijvoorbeeld voorheen kantooruren voldoende waren voor dienstverlening is nu vaak 7x24 uur de regel. Ook stellen klanten en partners in toenemende mate eisen aan risicomanagement en vragen zij om certificering, bijvoorbeeld voor transactieverwerking door dienstverleners (SAS70) of voor kwaliteit (ISO9000-serie). Zij kunnen aanzienlijke schade leiden als producten of dienstverlening niet, te laat, of met onvoldoende kwaliteit worden geleverd. Bovendien kunnen klanten hun leveranciers aansprakelijk stellen wanneer deze in gebreke blijven. Soms kan een bestuurder zelfs persoonlijk aan-

Ir. M. Gillard MBA is partner bij Verdonck, Klooster & Associates, onafhankelijk adviesbureau op het snijvlak van strategie, procesinrichting en ICT ([www.vka.nl](http://www.vka.nl)). [Marc.Gillard@vka.nl](mailto:Marc.Gillard@vka.nl). Drs. S. Debets MBA MSIT is managing consultant bij Verdonck, Klooster & Associates. [Steven.Debets@vka.nl](mailto:Steven.Debets@vka.nl).

sprakelijk worden gesteld indien hij/zij de risico's onvoldoende beheerst. Effectief risicomanagement levert een direct concurrentievoordeel op als de dienstverlening kritiek is voor de afnemende organisatie en de leverende organisatie bijvoorbeeld door certificering kan aantonen beter in control te zijn dan haar concurrenten. De AAA-status van Rabobank toont dit aan.

Een belangrijke drijfveer is ook het voorkomen van financiële, imago- en andere schade. Het belang van het voorkomen van imagoschade is recent wel aangetoond door de consequenties van een beschadigd imago voor Fortis. Ook gevolgschade neemt toe vanwege netwerk- en ketenafhankelijkheden tussen organisaties: wanneer uw leverancier onvoldoende kwaliteit levert komt ook de kwaliteit van uw product in gevaar. Denk aan het recente schandaal rondom het verontreinigde Chinese melkpoeder dat in verschillende producten is verwerkt. De kans op schade neemt toe en is lastiger in te schatten doordat de complexiteit van bedrijfsprocessen en de technologie die hiervoor wordt ingezet toeneemt.

De toenemende eisen vanuit wet- en regelgevers zijn vaak de directe aanleiding voor een organisatie om risicomanagement te professionaliseren. Sarbanes-Oxley (SOx), Basel-2, Solvency II en Tabaksblat zijn slechts enkele recente voorbeelden van toenemende regelgeving. Waar vroeger een mededeling dat de risico's onder controle zijn

voldoende was ('tell me'), zijn we via een fase van het aantonen van het 'in control' zijn ('show me') gekomen op een punt waar een organisatie daadwerkelijk moet bewijzen de risico's te beheersen ('prove me'). Risicomanagement staat derhalve terecht hoog op de managementagenda.

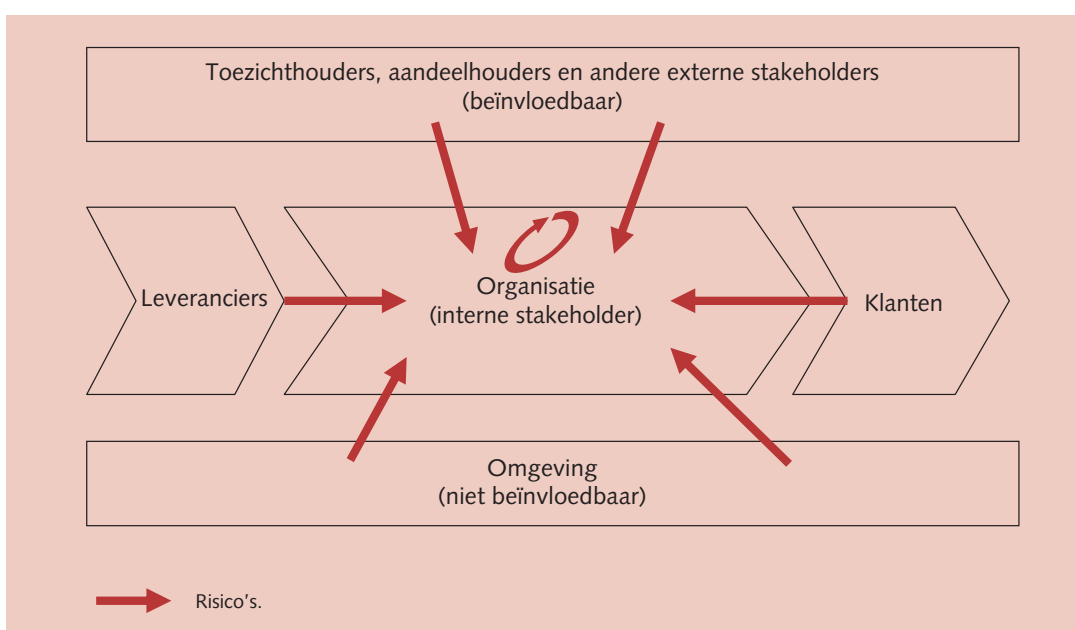
### Risico's bedreigen winstgevendheid

Vanuit verschillende kanten wordt de waardeketen van een organisatie bedreigd. In figuur 1 is dit grafisch weergegeven.

De waardecreatie van een organisatie kan op vele manieren worden verstoord. Leveranciers leveren niet, niet tijdig of van onvoldoende kwaliteit. Een recent voorbeeld is het kinderspeelgoed dat met giftige verf is geproduceerd. Het gevolg was een dure terugroepactie. Klanten kunnen besluiten geen producten of diensten meer af te nemen of niet (tijdig) te betalen. Als een van de eerste gevolgen van de kredietcrisis stonden in september 2007 in Groot-Brittannië voor de filialen van de bank Northern Rock lange rijen met klanten die hun geld met spoed wilden weghalen.

Toezichthouders kunnen vanuit maatschappelijke ontwikkelingen de regelgevingdruk verhogen waardoor de kosten voor 'compliance' stijgen. Voorbeelden zijn de introductie van SOx na boekhoudschandalen, en de roep om stringente regelgeving voor de banken als gevolg van de kredietcrisis.

**Figuur 1. Risico's voor de waardeketen**



Ook kan onvoldoende maatschappelijk bewust ondernemen een boycot tot gevolg hebben. Zo riep bijvoorbeeld in 2005 president Néstor Kirchner van Argentinië op tot een boycot van Shell om de stijging van de benzineprijs te beperken.

Professioneel risicomanagement helpt organisaties bij het verkrijgen en behouden van het vertrouwen van de belangrijkste stakeholders en zorgt ervoor dat zij voorbereid zijn wanneer risico's zich werkelijk manifesteren. Organisaties lopen echter tegen een belangrijk knelpunt aan bij de inrichting van risicomanagement: het silodilemma.

### Het silodilemma

Veel organisaties constateren nu dat zij onvoldoende aandacht hebben besteed aan het integraal beheersen van hun risico's. Afzonderlijke organisatieonderdelen hebben verantwoordelijkheid genomen en raamwerken ontwikkeld om de risico's vanuit hun specifieke functionele gebied te beheersen. Denk hierbij aan de CFO-office die financiële risico's beheerst, de HR-functie die zorgt dat een organisatie betrouwbare medewerkers heeft en de IT-functie die de risico's rondom informatievoorziening beheerst. Een dergelijke aanpak leidt tot het silodilemma: om risico's goed te beheersen worden ze binnen de individuele organisatiefuncties gemanaged omdat daar de noodzakelijke kennis aanwezig is. Bij deze aanpak ontbreekt echter het integrale overzicht van de 'risicoblootstelling' op organisatieniveau en worden risicobeperkende maatregelen niet op elkaar afgestemd. Als gevolg van het silodilemma is risicobeheersing vaak slechts beperkt effectief, met ook nog eens te hoge kosten.

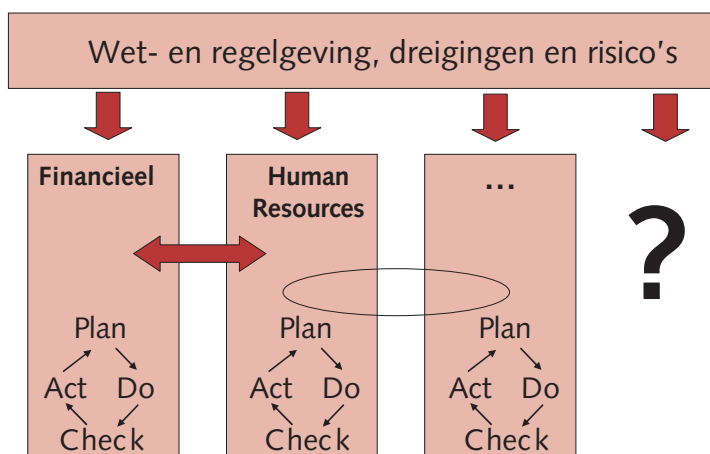
Uit het silodilemma (Figuur 2) kunnen we aantal knelpunten afleiden. In de eerste plaats kan er overlap tussen of juist een blinde vlek in de onderkende risico's ontstaan, omdat de desbetreffende risico's door meer organisatieonderdelen of juist door geen enkel organisatieonderdeel worden onderkend. Daarnaast hanteert ieder organisatieonderdeel zijn eigen losstaande governance-structuur. Deze structuren sluiten niet op elkaar aan en creëren onduidelijkheid in verantwoordelijkheden, vooral in het geval van een crisis of incident. Bovendien hanteren de silo's vaak een eigen 'risicotaal', wat de uitwisseling van managementinformatie over risico's tussen organisatieonderdelen niet ten goede komt. Hierdoor ontbreekt het beeld van de totale risicoblootstelling op organisatieniveau. Tot slot kan het silodilemma leiden tot een 'overkill' aan maatregelen: organisatieonderdelen proberen alle mogelijke wet- en regelgeving expliciet af te dekken binnen de interne processen en verliezen het doel van 'compliance' – aantoonbaar in control zijn – hierbij uit het oog. Zonder centrale sturing leidt dit tot aanzienlijke procesmatige inefficiënties en te hoge kosten.

**Als gevolg van het silodilemma is risicobeheersing vaak slechts beperkt effectief, met ook nog eens te hoge kosten**

### Integraal risicomanagement

Een aantal grotere organisaties heeft de eerste stappen gezet richting integrale risicobeheersing, echter de praktijk is weerbarstig. De oplossing voor het geschetste dilemma is een integrale visie op

Figuur 2. Het silodilemma



risicomanagement, met top-down afstemming tussen de verschillende functionele silo's. Wij duiden dit aan met 'Enterprise Risk Awareness' (ERA). 'Enterprise Risk Awareness' houdt in dat een organisatie bewust is ingericht op het integraal beheersen van de risico's. Organisaties bestaan uit processen, mensen, cultuur, technologie en andere middelen. Deze componenten zijn in het geval van ERA risicobewust ontworpen en risicobeheersende maatregelen maken daarbij een integraal onderdeel van het ontwerp uit. ERA betekent voor bedrijfsprocessen dat zij niet alleen zijn ontworpen vanuit de doelstelling een resultaat op te leveren, maar ook vanuit de noodzaak de risico's in het proces te managen. Als risicomanagement bij het ontwerpen van een bedrijfsproces wordt meegenomen ('by design'), voorkomt dat hoge kosten voor het achteraf implementeren van risicobeperkende maatregelen ('retrofit').

Ook medewerkers moeten 'risk aware' zijn. Bij het inrichten van een organisatie kunnen activiteiten niet of juist wel gecombineerd worden afhankelijk van de hiermee samenhangende risico's. Bijvoorbeeld, in het hele HR-proces van aanname tot en met ontslag is risicomanagement een integraal onderdeel. Dit betekent screening en zorgvuldige opleiding van personeel in gevoelige functies. Managers van een operationeel proces toetsen vanzelfsprekend of hun medewerkers voor hun functie gescreend zijn en zorgen dat zij over voldoende op-

leiding beschikken. Ook zorgen zij voor periodieke interne controles en functiescheiding bij fraudegevoelige financiële processen. In aansluiting op de functiescheidingen moet de ICT-functie het risicomanagement ondersteunen door het beperken van de bevoegdheden van medewerkers in computersystemen.

Een 'risk aware'-cultuur is hier nauw mee verbonden. Dit is een cultuur waarin het vanzelfsprekend is om over risico's na te denken, waarin medewerkers een risico melden aan de juiste functionaris zodra zij dit constateren en ook een cultuur waarin ethische waarden en normen centraal staan. ERA is een integrale benadering van risicomanagement, waarbij over de grenzen van elk organisatieonderdeel heen gekeken wordt. Dit kan alleen worden bereikt door top-down afstemming van het risicomanagement tussen organisatieonderdelen. Alleen met commitment en sturing vanuit de top van een organisatie kunnen risico's echt integraal worden gemanaged.

Managers 'verdrinken' in de richtlijnen voor risicomanagement die vanuit verschillende functionele gebieden worden opgelegd. Afstemming van deze richtlijnen helpt het lijnmanagement efficiënt en effectief aan de richtlijnen te voldoen. Dit betekent overigens niet dat elk organisatieonderdeel de risico's op precies dezelfde wijze moet managen. Voor bijvoorbeeld het beheersen van financiële risico's en informatierisico's zijn methoden in gebruik die

**Figuur 3. Integrale visie op risicomanagement: Enterprise Risk Awareness**



voor het specifieke gebied prima voldoen. Echter, in de praktijk hanteren veel organisatieonderdelen hun eigen taal voor risicomanagement met als gevolg misverstanden en dubbel werk. Dit compliceert kennisdelen en het interpreteren van rapportages.

In Figuur 3 is ERA schematisch weergegeven met de belangrijkste onderwerpen. De Risicostrategie is gericht op de risicotolerantie van een organisatie: welke risico's neemt een organisatie en welke risico's moeten worden afgedekt? Risicomanagement is gericht op het in kaart brengen en structureel beheersen van de risico's conform een standaard 'plan-do-check-act'-proces. Risicobeheersing toetst enerzijds of de Risicostrategie nog actueel is, anderzijds ook of de onderdelen van risicomanagement nog steeds goed functioneren. De kern van ERA bestaat uit risico-governance: een top-down integrale sturing op de voorgaande onderwerpen, waarbij afstemming tussen de verschillende silo's essentieel is.

### Concrete handvatten richting integraal risicomanagement.

Succesvolle invoering van 'Enterprise Risk Awareness' vereist een gestructureerde aanpak. Figuur 4 geeft de aanpak weer die een organisatie kan hanteren voor het invoeren van ERA.

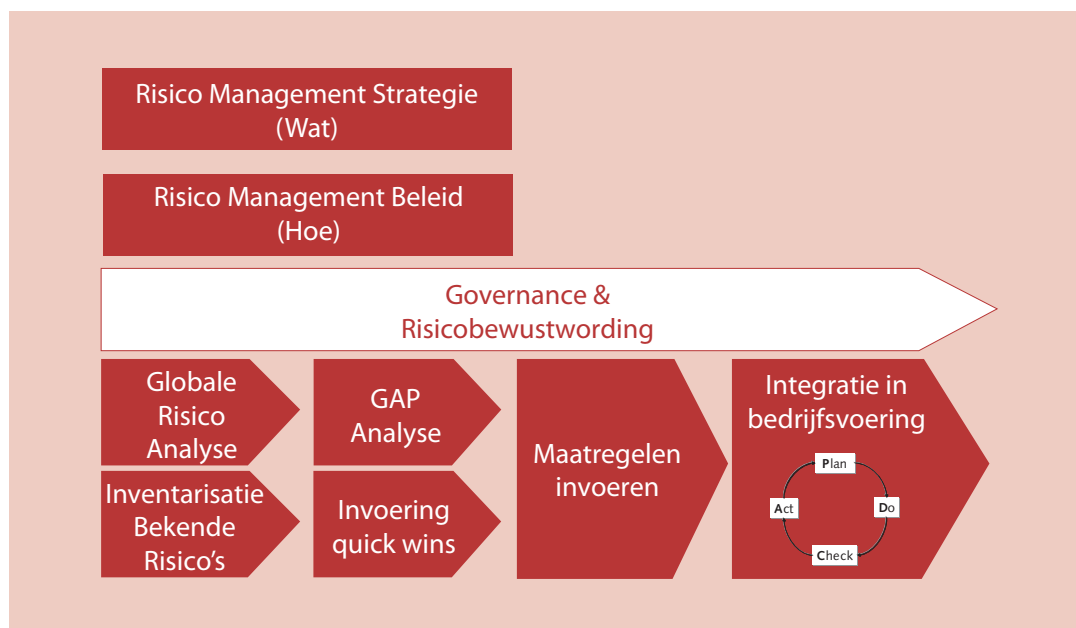
De eerste stap in het invoeringsproces is het opstel-

len en uitdragen van een geïntegreerde strategie voor risicomanagement, waarin het topmanagement onder andere het belang van goed risicomanagement voor de organisatie aangeeft en hier de doelstellingen voor specificeert. De strategie is overkoepelend voor de inrichting van risicomanagement binnen de individuele organisatieonderdelen en gaat uit van een geïntegreerde aanpak op concernniveau met daaronder een functionele verbijzondering naar organisatieonderdeel. Hierdoor worden zowel de kracht van integratie als de sterke punten van de verschillende functionele aanpakken benadrukt.

Verder specificeert het management in de strategie de risicotolerantie van de organisatie als geheel: welk risiconiveau is de organisatie bereid te accepteren? De strategie wordt door het management vervolgens verder uitgewerkt in een beleid voor risicomanagement. In dit beleid komt minimaal aan de orde op welke manier de organisatie het risicomanagement integraal aanstuurt (governance), hoe het risicobewustzijn van medewerkers wordt verhoogd (bewustwording) en hoe risicobeperkende maatregelen worden genomen en tussen organisatieonder-

**Enterprise Risk Awareness houdt in dat een organisatie bewust is ingericht op het integraal beheersen van de risico's**

**Figuur 4. Aanpak voor de invoering van ERA**



delen worden afgestemd. Het is essentieel dat het beleid wordt opgezet vanuit een integrale visie op risicomanagement. Een nuttig hulpmiddel bij het vaststellen van het beleid rondom risicobeperkende maatregelen is de kwetsbaarheidmatrix (Figuur 5).

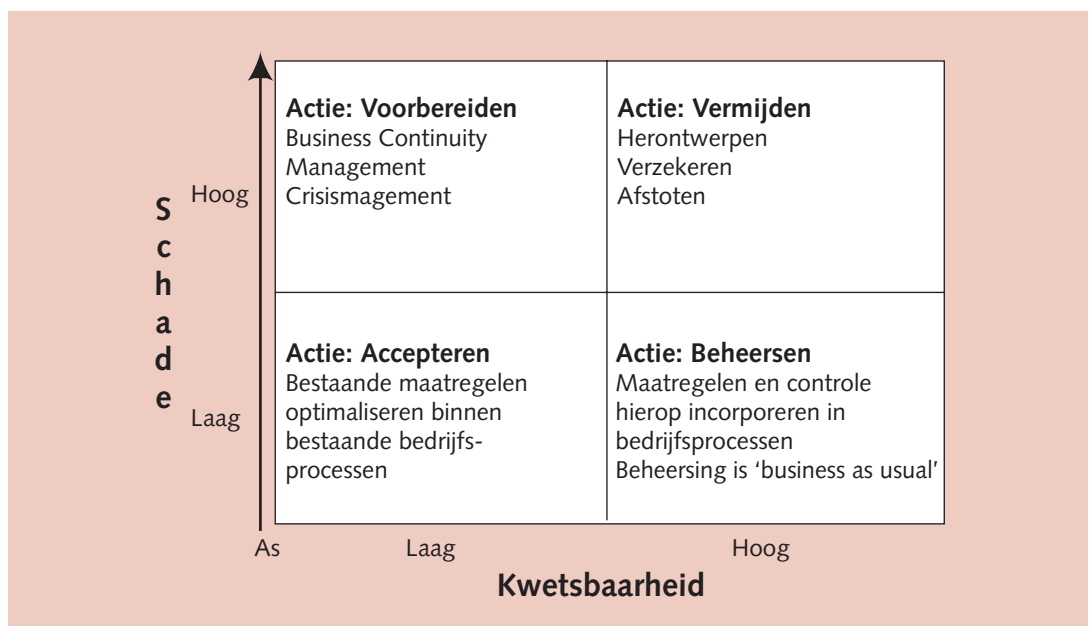
De kwetsbaarheidmatrix geeft duidelijk aan op welke manier organisaties hun kwetsbaarheden kunnen beheersen. De kwetsbaarheid betreft de kans dat een dreiging optreedt gegeven de maatregelen die een organisatie al heeft getroffen. Vrijwel geen enkele organisatie is immers een 'green field', waarbij de kans op een dreiging relevant is zonder rekening te houden met bestaande maatregelen. Risico's waarvoor de organisatie zeer kwetsbaar is en die kunnen leiden tot een hoge schade kunnen bijvoorbeeld worden behandeld door a) het nemen van risicoverminderende maatregelen, of b) verzekeren tegen het risico, of c) het afstoten van de betreffende bedrijfsactiviteit. Op strategisch niveau worden kwetsbaarheden op hun impact op de organisatie als geheel bekeken en niet in het licht van hun impact op een organisatieonderdeel. Zo kan een potentieel verlies van 1 miljoen euro voor een organisatieonderdeel een zeer groot risico inhouden, terwijl deze 'value-at-risk' op corporate niveau veel minder significant is. Het invoeringsproces zelf start met het inrichten van de overkoepelende besturing van risicomanagement en het opstarten van activiteiten om

het risicobewustzijn van de organisatie als geheel te vergroten. Aan de hand van een bedrijfsbrede globale risicoanalyse bepaalt de organisatie haar ('high level') risicoprofiel. Dit risicoprofiel wordt vervolgens met behulp van een GAP Assessment (verschillenanalyse) tegen de bestaande maatregelen gespiegeld, op basis waarvan een maatregelenplan wordt opgesteld en uitgevoerd. De uitvoering zal zowel op corporate niveau als binnen de individuele bedrijfsonderdelen plaatsvinden.

Parallel aan dit proces definieert de organisatie op basis van de globale risicoanalyse een aantal 'quick wins'. Deze zullen vaak voortkomen uit bekende risico's c.q. kwetsbaarheden en stellen de organisatie in staat om snel voortgang te boeken met het beheersen van de belangrijkste risico's, terwijl de gestructureerde aanpak van de overige risico's gewoon doorgang vindt.

Het invoeren van een uniforme rapportagemethodiek vanaf de start van het project is essentieel voor een succesvolle geïntegreerde aanpak. Traditioneel zullen de verschillende organisatieonderdelen een eigen analyse- en rapportagemethodiek hebben voor risico's. Via uniformering van de rapportage wordt het topmanagement in een vroeg stadium betrokken bij het geïntegreerde risicomanagement en wordt zij in staat gesteld te sturen op een risicoportefeuille in plaats van op individuele kwetsbaarheden. De geïntegreerde rapportage wordt gebaseerd op een uniforme 'risicotaal' (definities

**Figuur 5. Kwetsbaarheidmatrix**



en taxonomieën) die de specifieke risicoterminologie van organisatieonderdelen afschermt voor het topmanagement.

Het invoeren van risicomanagement wordt afgesloten met de integratie van risicomanagement in de bedrijfsvoering van de organisatie. Risicomanagement wordt hierdoor integraal onderdeel van de business en daardoor 'business-as-

usual'. Uiteindelijk resulteert deze aanpak in een integrale beheersing van de risicoportefeuille van een organisatie. 'Enterprise Risk Awareness' helpt het management de essentie van hun business te doorgronden: waardoor wordt mijn business beïnvloed en hoe kan ik dit beheersen? De huidige roerige tijden tonen wel aan dat het integraal beheersen van risico's harde noodzaak is.