

ferma



FEDERATION OF
EUROPEAN RISK
MANAGEMENT
ASSOCIATIONS

DE RISK MANAGEMENT NORM





Inleiding

De Risk Management Standard of norm voor risicobeheer is het gezamenlijke werk van de belangrijkste risicobeheersorganisaties in het Verenigd Koninkrijk, met name het Institute of Risk Management (IRM), de Association of Insurance and Risk Managers (AIRMIC) en ALARM, het nationale forum voor risicobeheer in de overheidssector.

Gedurende een lange periode van overleg heeft het team getracht de ideeën en meningen te achterhalen van tal van andere beroepsorganisaties met belangen in risicobeheer.

Risicobeheer is een snel groeiende discipline en er zijn vele en verschillende opvattingen en beschrijvingen van wat risicobeheer inhoudt, hoe het dient te worden verwezenlijkt en waartoe het dient. Een zekere mate van normering is noodzakelijk om verzekerd te zijn van een passend(e) :

- *terminologie betrekking hebbend op gebruikte teksten*
- *proces waarlangs het risicobeheer kan worden uitgevoerd*
- *een organisatiestructuur voor risicobeheer*
- *doelstelling van risicobeheer*

Belangrijk daarbij is dat de norm zowel de positieve als de negatieve kanten van risico onderkent.

Risicobeheer is niet alleen iets voor ondernemingen of overheidsinstellingen, maar voor elke activiteit zowel op korte als lange

termijn. De voordelen en kansen dienen niet alleen in de context van de activiteit zelf te worden gezien, maar ook in relatie met de vele en verschillende 'partijen' die erbij betrokken kunnen zijn.

Er zijn vele manieren om de doelstellingen van risicobeheer te bereiken en het zou onmogelijk zijn om ze allemaal uiteen te zetten in een enkel document. Vandaar dat het nooit de bedoeling was om een dicterende norm te produceren die uiteindelijk geleid zou hebben tot een checklist benadering of een certificeerbaar proces. Het voldoen aan de verschillende samenstellende delen van de norm, zij het op verschillende manieren, geeft organisaties de mogelijkheid te verklaren dat de norm wordt nageleefd. De norm vertegenwoordigt de 'best practice' waaraan de organisaties zich kunnen meten.

Waar mogelijk heeft de norm gebruik gemaakt van de terminologie inzake risicobeheer vastgelegd door de Internationale Organisatie voor Normalisatie (ISO) in haar recente document ISO/IEC Guide 73 Risk Management - Vocabulary - Guidelines for use in standards.

Gezien de snelle ontwikkelingen op dit gebied wordt feedback van organisaties naarmate ze de norm toepassen op prijs gesteld door de auteurs (zie achterzijde van deze Gids voor adressen). Het is de bedoeling om de norm geregeld aan te passen aan de 'best practice'.



1. Risico

Risico kan worden omschreven als de combinatie van de waarschijnlijkheid van een gebeurtenis en de gevolgen ervan (ISO/IEC Guide 73).

In alle soorten organisaties bestaat de mogelijkheid dat gebeurtenissen en gevolgen een mogelijkheid voor winst (positief) of een dreiging tot verlies (negatief) vertegenwoordigen.

Risicobeheer wordt in toenemende mate erkend als een proces dat rekening houdt met zowel de positieve als negatieve aspecten van risico. Om die reden beschouwt deze norm risico vanuit de beide gezichtspunten.

Op het vlak van veiligheid is het algemeen erkend dat gevolgen alleen negatief kunnen zijn. Vandaar dat het beheer van veiligheidsrisico's gericht is op de preventie en de beperking van schade.

2. Risicobeheer

Risicobeheer vormt een centraal onderdeel van het strategische beheer van elke organisatie. Het is het proces waarmee organisaties de risico's verbonden aan hun activiteiten methodisch aan de orde stellen met de bedoeling om binnen elke activiteit en over de totale portefeuille van activiteiten een duurzaam voordeel te bereiken.

Goed risicobeheer is toegespitst op de identificatie en de behandeling van die risico's. Het is de bedoeling om zoveel mogelijk duurzame waarde aan alle activiteiten van de organisatie toe te voegen. Het ordent het inzicht in de potentiële positieve en negatieve aspecten van alle factoren die de organisatie kunnen beïnvloeden. Het vergroot de kans op succes en verkleint zowel de kans op falen en

de onzekerheid rond het al dan niet behalen van de algemene doelstellingen van de organisatie.

Risicobeheer dient een continu en evoluerend proces te zijn dat in alle opzichten geldt voor de strategie van de organisatie en de uitvoering van die strategie. Het dient systematisch alle risico's die verband houden met de activiteiten van de organisaties uit het verleden, het heden en vooral de toekomst aan de orde te stellen.

Het dient geïntegreerd te zijn in de cultuur van de organisatie door middel van een effectief beleid en een programma dat geleid wordt door het topmanagement. Het dient de strategie te vertalen in tactische en operationele doelstellingen door in heel de organisatie verantwoordelijkheden toe te wijzen, waarbij elke leidinggevende en werknemer verantwoordelijk is voor risicobeheer als onderdeel van de functieomschrijving. Het ondersteunt verantwoordelijkheid, prestatiemeting en beloning, en stimuleert zo de operationele doeltreffendheid op alle niveaus.

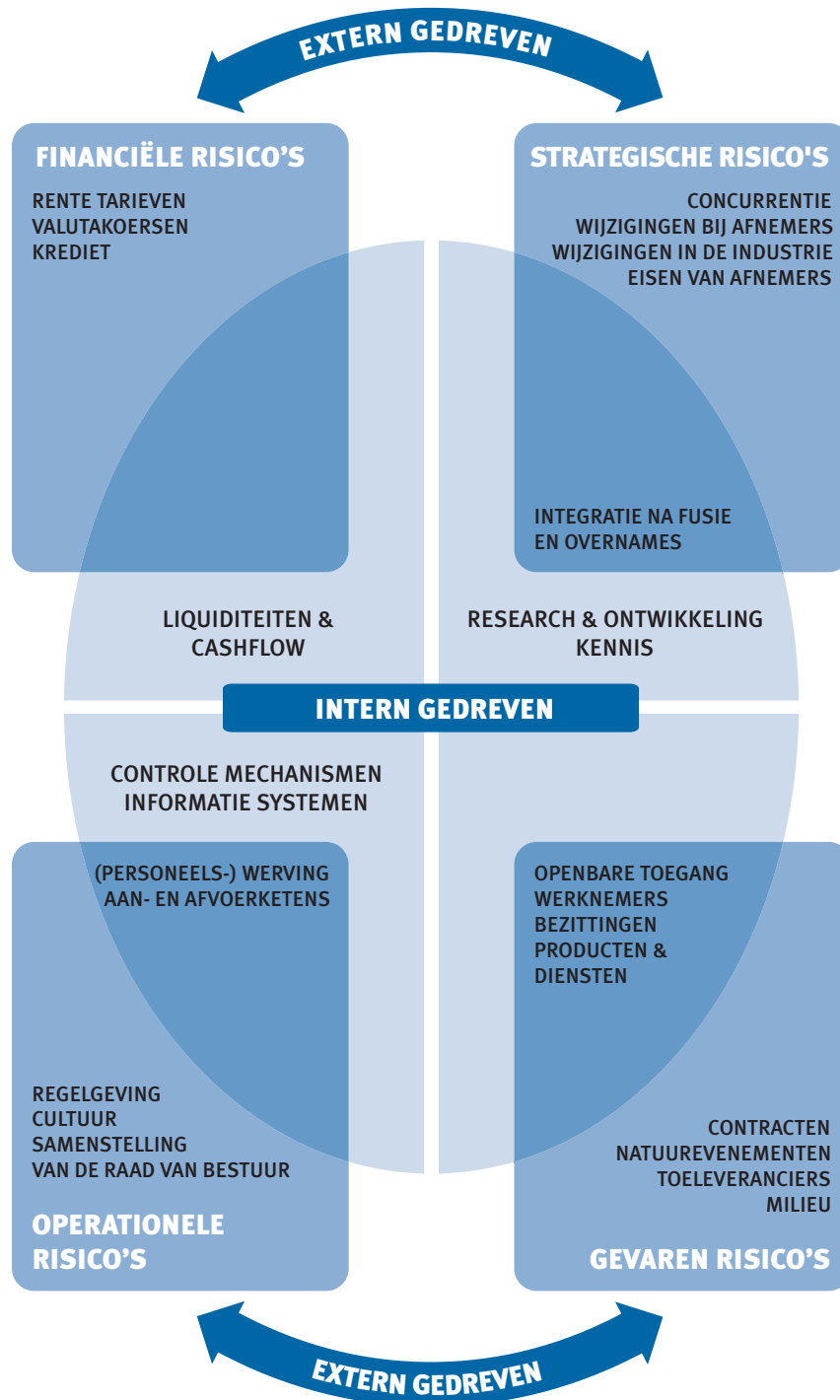
2.1 Externe en interne factoren

De risico's waarmee een organisatie en haar activiteiten te maken hebben, kunnen voortvloeien uit factoren die zowel binnen als buiten de organisatie liggen.

De grafiek op de volgende pagina vat enkele voorbeelden samen van de voornaamste risico's in die gebieden en toont aan dat aan sommige specifieke risico's zowel externe als interne factoren ten grondslag kunnen liggen, waardoor de risico's de twee gebieden overlappen. De risico's kunnen verder in categorieën worden ondergebracht zoals strategisch, financieel, operationeel, gevaar, enz.

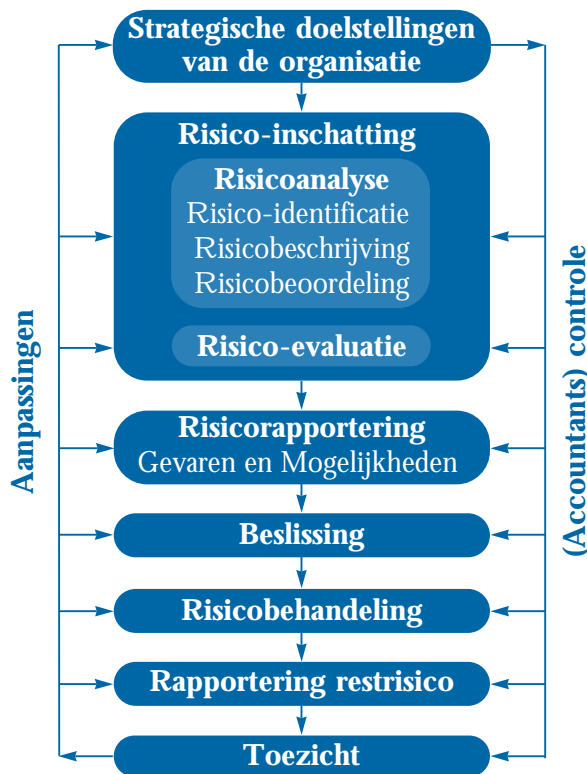


2.1 Voorbeelden van de drijvende factoren van de voornaamste risico's





2.2 Het risicobeheersproces



Risicobeheer beschermt en voegt waarde toe aan de organisatie en haar 'partijen' door de doelstellingen van de onderneming te ondersteunen door:

- aan een organisatie een structuur te bieden aan de hand waarvan toekomstige activiteiten kunnen plaatsvinden op een consistente en gecontroleerde manier
- het besluitvormingsproces, de planning en de prioritering te verbeteren door een breed en gestructureerd inzicht in de bedrijfsactiviteit, de volatiliteit en de opportuniteit/het gevaar van een project
- bij te dragen tot een efficiënter gebruik/toewijzing van kapitaal en middelen binnen de onderneming
- de volatiliteit in de niet-essentiële gebieden van de onderneming te verminderen
- de bezittingen en het bedrijfsimago te beschermen en te versterken
- het ontwikkelen en ondersteunen van personeel en het kennisbestand van de onderneming
- de operationele effectiviteit te optimaliseren



3. Risicobeoordeling

Risico-inschatting wordt door de ISO/IEC Guide 73 omschreven als het overkoepelende proces van risicoanalyse en risicobeoordeling. (zie bijlage)

4. Risicoanalyse

4.1 Risico-identificatie

Risico-identificatie tracht de blootstelling van een organisatie aan onzekerheid te identificeren. Daarvoor is een grondige kennis vereist van de organisatie, de markt waarin de organisatie werkzaam is, en de juridische, sociale, politieke en culturele omgeving waarin de organisatie existeert, alsmede de ontwikkeling van een goed inzicht in de strategische en operationele bedrijfsdoelstellingen, waaronder de kritische succesfactoren van die doelstellingen en de gevaren en opportuniteiten die verband houden met de verwezenlijking ervan.

Risico-identificatie dient op een systematische manier te worden aangepakt zodat alle belangrijke activiteiten binnen de organisatie geïdentificeerd kunnen worden en alle risico's voortvloeiend uit die activiteiten afgebakend kunnen worden. Alle verwante volatiliteit met betrekking tot die activiteiten dient te worden geïdentificeerd en gecategoriseerd.

Bedrijfsactiviteiten en -besluiten kunnen op verschillende manieren worden ingedeeld, zoals bijvoorbeeld:

- *Strategisch - betreft de strategische doelstellingen van de organisatie op lange termijn. Zij kunnen beïnvloed worden door factoren als beschikbaarheid van kapitaal, soevereine en politieke risico's, wettelijke en regelgevende wijzigingen, reputatie en veranderingen in de fysieke omgeving*
- *Operationeel – betreft de dagelijkse aangelegenheden waarmee de organisatie wordt geconfronteerd terwijl zij haar strategische doelstellingen tracht te behalen*
- *Financieel – betreft het effectief beheer van en toezicht op de financiën van de organisatie en de effecten van externe factoren zoals*

beschikbaarheid van krediet, wisselkoersen, rentebewegingen en andere marktblootstellingen

- *Kennisbeheer – betreft het doeltreffend beheer van en toezicht op de kennismiddelen, alsook de totstandbrenging, bescherming en communicatie ervan. Externe factoren omvatten onder meer het ongeoorloofde gebruik of misbruik van intellectuele eigendom, stroomstoringen in het net en concurrerende technologie. Mogelijke voorbeelden van interne factoren zijn systeemstoring of verlies van belangrijk personeel.*
- *Naleving (van wet en regelgeving) – betreft zaken zoals veiligheid en gezondheid, milieu, handelsvoorschriften, consumentenbescherming, gegevensbescherming, werkaangelegenheden en regelgevende zaken*

Hoewel de risico-identificatie kan worden uitgevoerd door externe consultants, zal een interne benadering aan de hand van duidelijk gecommuniceerde, consistente en gecoördineerde processen en hulpmiddelen (zie bijlage, pagina 14) doorgaans effectiever zijn. Intern 'ownership' van het risicobeheersproces is van essentieel belang.

4.2 Risicobeschrijving

Het doel van de risicobeschrijving is de geïdentificeerde risico's weer te geven in een gestructureerde indeling, bijvoorbeeld door middel van een tabel. De risicobeschrijvingstabel op de volgende pagina kan worden gebruikt om de beschrijving en inschatting van de risico's te vergemakkelijken. Het gebruik van een goed ontworpen structuur is nodig om een uitvoerige risico-identificatie, -beschrijving en -inschatting te garanderen. Door rekening te houden met het gevolg en de waarschijnlijkheid van elk van de risico's uiteengezet in de tabel, moet het mogelijk zijn om de voornaamste risico's die meer in detail geanalyseerd dienen te worden, te prioriteren. De identificatie van de risico's gekoppeld aan de bedrijfsactiviteiten en het besluitvormingsproces kunnen worden gecategoriseerd als strategisch, projectgebonden/tactisch en operationeel. Het is belangrijk om het risicobeheer niet alleen in de beginfase van een project te integreren, maar ook tijdens de eigenlijke verwezenlijking ervan.



4.2.1 Tabel - Risicobeschrijving

1. Benaming van het risico	
2. Draagwijdte van het risico	Kwalitatieve beschrijving van de gebeurtenissen, hun omvang, type, aantal en afhankelijkheid
3. Aard van het risico	bijv. strategisch, operationeel, financieel, kennis of naleving van wet en regelgeving
4. 'stakeholders'	'stakeholders' en hun verwachtingen
5. Risicoweging	Belang en waarschijnlijkheid
6. Risicotolerantie	Kans op verlies en financiële impact van het risico Value at risk Waarschijnlijkheid en omvang van de potentiële verliezen/winsten Doelstelling(en) voor controle van het risico en gewenst prestatieniveau
7. Risicobehandeling & controlemechanismen	Basismiddelen aan de hand waarvan het risico momenteel wordt beheerd Betrouwbaarheidsniveaus van bestaande controle Identificatie van protocollen voor toezicht en revisie
8. Potentiële maatregel voor verbetering	Aanbevelingen om risico te verkleinen
9. Strategie en beleidsontwikkelingen	Identificatie van de functie verantwoordelijk voor het ontwikkelen van de strategie en het beleid

4.3 Risicoschatting

Risicoschatting kan kwantitatief, semi-kwantitatief of kwalitatief zijn ten opzichte van de waarschijnlijkheid dat de gebeurtenis zal plaatsvinden en het mogelijke gevolg ervan.

Gevolgen kunnen bijvoorbeeld in termen van zowel gevaar (negatief risico) als opportuniteiten (positief risico) hoog, middelmatig of laag zijn (zie tabel 4.3.1).

Waarschijnlijkheid kan hoog, middelmatig of laag zijn maar vereist verschillende definities met betrekking tot gevaren en opportuniteiten (zie tabellen 4.3.2 en 4.3.3).

Voorbeelden zijn gegeven in de tabellen op de volgende pagina. De maatstaven van gevolg en waarschijnlijkheid kunnen verschillen van de ene tot de andere organisatie.

Heel wat organisaties vinden bijvoorbeeld dat het inschatten van gevolg en waarschijnlijkheid als zijnde hoog, middelmatig of laag ruim voldoet aan hun behoeften en in een 3x3-matrix kan worden voorgesteld.

Andere organisaties vinden dan weer dat het inschatten van gevolg en waarschijnlijkheid door middel van een 5x5-matrix voor hen het beste resultaat oplevert.

**Tabel 4.3.1 Gevolgen - Zowel dreigingen als mogelijkheden**

Hoog	De financiële impact op de organisatie zal naar alle waarschijnlijkheid hoger zijn dan €x Belangrijke impact op de strategie of operationele activiteiten van de organisatie Belangrijke bezorgdheid van “partijen”
Middelmatig	De financiële impact op de organisatie zal vermoedelijk tussen €x en €y schommelen Matige impact op de strategie of operationele activiteiten van de organisatie Matige bezorgdheid van “partijen”
Laag	De financiële impact op de organisatie zal naar alle waarschijnlijkheid lager zijn dan €x Lage impact op de strategie of operationele activiteiten van de organisatie Lage bezorgdheid van “partijen”

Tabel 4.3.2 Kans van optreden – Gevaren

Schatting	Beschrijving	Indicatoren
Hoog (Waarschijnlijk)	Zal naar alle waarschijnlijkheid elk jaar plaatsvinden of meer dan 25% kans van optreden.	Mogelijkheid dat de gebeurtenis zich meerdere keren binnen de periode van tijd voordoet (bijvoorbeeld - tien jaar) Heeft zich recent voorgedaan.
Middelmatig (Mogelijk)	Zal naar alle waarschijnlijkheid in een periode van tien jaar plaatsvinden of minder dan 25% kans van optreden.	Zou meer dan een keer binnen de periode van tijd kunnen plaatsvinden (bijvoorbeeld - tien jaar). Is moeilijk te beheersen als gevolg van een aantal externe invloeden. Bestaat er een historiek van het gebeuren?
Laag (Gering)	Zal waarschijnlijk niet plaatsvinden in een periode van tien jaar of minder dan 2% kans van optreden.	Heeft zich nog niet voorgedaan Zal waarschijnlijk niet plaatsvinden .



Tabel 4.3.3 Kans van optreden - Mogelijkheden

Schatting	Beschrijving	Indicatoren
Hoog (Waarschijnlijk)	Gunstig resultaat zal naar alle waarschijnlijkheid worden behaald in een jaar of meer dan 75% kans van optreden.	Duidelijke opportuniteit waarop kan worden vertrouwd met redelijke zekerheid, op korte termijn te behalen op grond van de huidige beheersprocessen.
Middelmatig (Mogelijk)	Redelijke vooruitzichten op gunstige resultaten in een jaar of 25% tot 75% kans van optreden.	Opportunities die haalbaar zijn maar een voorzichtig beheer vereisen. Opportunities die boven de planning kunnen uitkomen.
Laag (Gering)	Enige kans van gunstig resultaat op halflange termijn of minder dan 25% kans van optreden.	Mogelijke opportuniteit die nog volledig onderzocht dient worden door het management. Opportuniteit waarvoor de kans op succes laag is op grond van de beheersmiddelen die momenteel toegepast worden.

4.4 Methoden en technieken voor risicoanalyse

Om de risico's te analyseren, kunnen verschillende technieken worden gebruikt. Die technieken kunnen kenmerkend zijn voor het positieve risico of het negatieve risico of kunnen voor beiden worden aangewend. (zie *bijlage*).

4.5 Risicoprofiel

Aan de hand van het resultaat van de risicoanalyse kan een risicoprofiel worden aangemaakt dat aan elk risico een waardecijfer geeft en een hulpmiddel biedt aan de hand waarvan kan worden bepaald aan welke risico's eerst aandacht dient te worden besteed. Het resultaat van de risicoanalyse kan worden gebruikt om een risicoprofiel te vervaardigen waarbij een volgorde van belang aan elk risico kan worden toegekend en een

hulpmiddel wordt gegeven voor het vaststellen van de prioriteiten bij de risicobehandelingsinspanningen. Op die manier wordt elk geïdentificeerd risico gerangschikt en ontstaat een beeld van het relatieve belang.

Dankzij dit proces kan het risico voor het betreffende bedrijfs onderdeel in kaart worden gebracht, kan de geldende primaire beheersprocedure worden beschreven en kunnen de gebieden worden aangegeven waar het niveau van risicobeheer investeringen verhoogd, verlaagd of herverdeeld kan worden.

Het toekennen van verantwoordelijkheid bevordert dat het 'ownership' van het risico wordt erkend en dat het passende beheersmiddel wordt toegewezen.



5. Risicobeoordeling

Zodra de risicoanalyse voltooid is, dienen de geraamde risico's te worden vergeleken met risicocriteria die door de organisatie bepaald werden. De risicocriteria kunnen zowel verwante kosten en baten, wettelijke vereisten, sociaal-economische en milieufactoren, als 'stakeholders' interesses, enz. omvatten. De risicobeoordeling wordt bijgevolg gebruikt om beslissingen te nemen over het belang van de risico's voor de organisatie en om te bepalen of elk specifiek risico al dan niet dient te worden aanvaard of behandeld.

6. Risicobehandeling

Risicobehandeling is het proces van het selecteren en implementeren van maatregelen om het risico te wijzigen. Risicobehandeling kent als voornaamste elementen risicobeheersing/-beperking, maar strekt zich uit tot bijvoorbeeld risicovermijding, risico-overdracht, risicofinanciering, enz.

OPMERKING: in deze norm verwijst risicofinanciering naar de mechanismen (bijv. verzekeringsprogramma's) om de financiële gevolgen van het risico te financieren. Als risicofinanciering wordt doorgaans niet beschouwd het verschaffen van fondsen nodig om de kosten voor het in praktijk brengen van de risicobehandeling te dekken (zoals bepaald door ISO/IEC Guide 73).

Elk systeem van risicobehandeling dient op zijn minst te voorzien in:

- een effectieve en efficiënte uitvoering van de organisatie
- effectieve interne controlemaatregelen
- de naleving van wet en regelgeving

Het risicoanalyse proces draagt bij tot het effectief en efficiënt beheer van de organisatie door juist die risico's te identificeren waaraan het management aandacht dient te besteden. Zij zullen prioriteit dienen te geven aan risicobeheersmaatregelen met betrekking tot hun potentie om aan de organisatie ten goede te komen.

Effectiviteit van interne controle is de mate waarin het risico ofwel geëlimineerd ofwel verkleind zal worden door de voorgestelde controlemaatregelen.

Rendabiliteit van interne controle verwijst naar de kosten voor het implementeren van de controle vergeleken met de verwachte voordelen van de risicovermindering.

De voorgestelde controlemaatregelen dienen te worden gemeten in termen van potentieel economisch effect indien er geen actie wordt ondernomen vergeleken met de kosten van de voorgestelde maatregel(en), en vereisen stevast meer uitgebreide informatie en veronderstellingen dan onmiddellijk beschikbaar zijn.

In eerste instantie dienen de implementatiekosten te worden bepaald. Dit dient met enige precisie te worden berekend, aangezien op grond daarvan de rendabiliteit zal worden gemeten. Daarnaast dient ook het verlies te worden berekend dat verwacht wordt indien er geen maatregelen worden genomen. Door de resultaten te vergelijken, kan het management beslissen of de risicocontrolemaatregelen wel of niet zullen worden toegepast.

De naleving van wet en regelgeving is geen optie. Dat betekent dat een organisatie de toepasbare wetten dient te begrijpen en een systeem van controlemaatregelen dient uit te werken om de naleving van die wetten tot stand te brengen. Slechts nu en dan kan er enige flexibiliteit worden betracht wanneer de kosten voor het beperken van een risico volkomen onevenredig zijn aan dat risico.

Een methode voor het verkrijgen van financiële bescherming tegen de impact van risico's is risicofinanciering, waaronder begrepen verzekering. Echter dient men zich ervan bewust te zijn dat bepaalde verliezen of onderdelen van een verlies onverzekerbaar zijn bijvoorbeeld de onverzekerde kosten gekoppeld aan werkgerelateerde gezondheid, veiligheid of milieu-incidenten, die mede schade kunnen berokkenen aan de moraal van werknemers of aan de reputatie van de organisatie.



7. Risicoverslaglegging en -communicatie

7.1 Interne verslaglegging

De verschillende niveaus binnen een organisatie hebben behoefte aan verschillende informatie afkomstig uit het risicobeheerproces.

De Raad van Bestuur dient:

- kennis te hebben van de voornaamste risico's waaraan de organisatie blootstaat
- te weten wat de mogelijke effecten zijn op de aandeelhouderswaarde van afwijkingen op de verwachte prestatie
- passende niveaus van bewustzijn door heel de organisatie te garanderen
- te weten hoe de organisatie een crisis zal beheersen
- te weten wat het belang is van het vertrouwen van de 'stakeholders' in de organisatie
- te weten hoe te communiceren met de beleggersgemeenschap indien van toepassing
- ervan verzekerd te zijn dat het risicobeheerproces effectief werkt
- een duidelijk risicobeheerbeleid te publiceren dat de filosofie en de verantwoordelijkheden van het risicobeheer afdekt

De bedrijfsonderdelen dienen:

- bewust te zijn van de risico's die onder hun verantwoordelijkheid vallen, van de mogelijke impact die de risico's kunnen hebben op andere bedrijfsonderdelen en de uitwerkingen die andere bedrijfsonderdelen op hen kunnen hebben
- over prestatie-indicatoren te beschikken die hen in staat stellen om toezicht te houden

op de voornaamste bedrijfs- en financiële activiteiten, het toewerken naar doelstellingen en het identificeren van ontwikkelingen die interventie vereisen (bijv. verwachtingen en budgetten)

- over systemen te beschikken die op juiste tijdstippen afwijkingen in de budgetten en verwachtingen signaleren zodat de nodige maatregelen genomen kunnen worden
- systematisch en onmiddellijk verslag uit te brengen bij het topmanagement over waargenomen nieuwe risico's of gebreken in de bestaande controlemaatregelen

Individuele personen dienen:

- te begrijpen hoe ze kunnen zorg dragen voor het voortdurend verbeteren van het risicobeheerproces
- zich ervan bewust te zijn dat risicobeheer en risicobewustzijn een essentieel onderdeel zijn van de cultuur van de organisatie
- systematisch en onmiddellijk verslag uit te brengen aan het topmanagement over waargenomen nieuwe risico's of gebreken in de bestaande controlemaatregelen

7.2 Externe verslaglegging

Een onderneming dient op regelmatige tijdstippen verslag te doen aan haar 'stakeholders' over haar risicobeheerbeleid en de effectiviteit in het behalen van haar doelstellingen.

In toenemende mate vertrouwen 'stakeholders' erop dat organisaties bewijs leveren van een effectief beheer van de niet-financiële prestaties van de organisatie op het gebied van publieke aangelegenheden, mensenrechten, werkgerelateerde praktijken, gezondheid en veiligheid, en het milieu.



Een goed corporate governance vereist dat organisaties een methodische benadering van risicobeheer toepassen die:

- *de belangen van hun 'stakeholders' beschermt*
- *garandeert dat de Raad van Bestuur haar taken vervult ten aanzien van het leiding geven over de strategie, waarde creëert en toezicht houdt op het resultaat van de organisatie*
- *garandeert dat er beheerscontroles van kracht zijn die naar behoren werken*

De afspraken voor de formele rapportering over risicobeheer dienen duidelijk omschreven te zijn en toegankelijk te zijn voor alle 'stakeholders'.

De formele rapportering dient te behandelen:

- *de controlemethoden – in het bijzonder verantwoordelijkheden van het management voor risicobeheer*
- *de werkwijzen toegepast om de risico's te identificeren en hoe die werkwijzen worden aangepakt door de risicobeheerssystemen*
- *de voornaamste controlesystemen van kracht om belangrijke risico's te beheren*
- *het van kracht zijnde systeem voor controle en revisie*

Alle belangrijke gebreken aan het licht gebracht door het systeem, of in het systeem zelf, dienen te worden gemeld samen met de maatregelen om die gebreken aan te pakken.

8. De structuur en administratie van risicobeheer.

8.1 Risicobeheerbeleid

Bij het opstellen van een risicobeheerbeleid dient een organisatie haar benadering van en zin voor risico af te bakenen, alsook haar benadering ten opzichte van risicobeheer. Daarnaast dient het beleid ook te bepalen wie binnen de organisatie verantwoordelijk is voor risicobeheer.

Voorts dient het beleid ook te refereren aan de wettelijke vereisten waaraan beleidsverklaringen dienen te voldoen, bijv. op het gebied van gezondheid en veiligheid. Inherent aan het risicobeheer is een geheel van hulpmiddelen en technieken die toegepast kunnen worden in de verscheidene stadia van het bedrijfsproces.

Om effectief te kunnen zijn vereist het risicobeheerproces:

- *betrokkenheid van de algemene directeur en de topleidinggeveden van de organisatie*
- *toewijzing van de verantwoordelijkheden binnen de organisatie*
- *toewijzing van de geschikte middelen voor training en ontwikkeling van een groter risicobewustzijn door alle 'stakeholders'*

8.2 Rol van de Raad van Bestuur (Directie)

De Raad van Bestuur (Directie) is verantwoordelijk voor het bepalen van de strategische richting van de organisatie en voor het creëren van de omgeving en de structuren waarbinnen het risicobeheer doeltreffend kan functioneren.

Dat kan via een leidinggevende groep, een niet-leidinggevend comité, een auditcommissie of een dergelijke functie die past bij de werkwijze van de organisatie en in staat is om als een 'sponsor' voor risicobeheer op te treden.

De Raad van Bestuur (Directie) dient bij de beoordeling van haar systeem van interne controle op zijn minst rekening te houden met:

- *de aard en de omvang van de negatieve risico's die voor de organisatie aanvaardbaar zijn binnen haar specifieke activiteit*
- *de waarschijnlijkheid dat die risico's werkelijkheid worden*
- *de manier waarop dient te worden omgegaan met onaanvaardbare risico's*



- *het vermogen van de organisatie om de waarschijnlijkheid en de impact op haar activiteiten te minimaliseren*
- *de kosten en baten van het risico en de controlemaatregel die ondernomen werd*
- *de doeltreffendheid van het risicobeheerproces*
- *de risicodragende gevolgen van bestuursbesluiten*

8.3 Rol van de business units

Dit omvat het volgende:

- *de business units hebben de primaire verantwoordelijkheid voor het dagelijkse beheer van de risico's*
- *het management van de business unit is verantwoordelijk voor het bevorderen van het risicobewustzijn binnen de activiteit; het dient doelstellingen inzake risicobeheer in hun activiteit in te voeren*
- *risicobeheer dient een punt te zijn op de agenda van de vaste managementvergadering zodat aandacht wordt gegeven aan en er nieuwe prioriteiten kunnen worden gegeven aan het werk in het licht van een efficiënte risicoanalyse*
- *het management van de business unit dient ervoor te zorgen dat het risicobeheer geïntegreerd is in de conceptuele fase alsmede gedurende de looptijd van een project*

8.4 Rol van het risicobeheer

Functie

Afhankelijk van de grootte van de organisatie kan de risicobeheerfunctie variëren van een enkele 'risicovoorvechter', een parttime risicomanager tot een volledige risicobeheerafdeling.

De risicobeheerfunctie dient onder meer het volgende te omvatten:

- *uitwerken van een beleid en strategie voor risicobeheer*

- *voornaamste voorvechter van risicobeheer op strategisch en operationeel vlak*
- *ontwikkelen van een cultuur van risicobewustzijn binnen de organisatie, inclusief benodigde opleiding*
- *vastleggen van een intern risicobeleid en structuren voor de business units*
- *ontwerpen en herzien van processen voor risicobeheer*
- *coördineren van de verschillende functionele activiteiten die advies verlenen over risicobeheerkwesties binnen de organisatie*
- *uitwerken van risicoresponsmethoden, waaronder rampen- en bedrijfscontinuïteitsplannen*
- *voorbereiden van risicoverslagen voor de Raad van Bestuur en de 'stakeholders'*

8.5 Rol van de Interne Audit

De rol van de Interne Audit is doorgaans verschillend naargelang de organisatie.

In praktijk kan de rol van Interne Audit bestaan uit sommige of alle hierna genoemde elementen:

- *de interne audit activiteiten focussen op de belangrijke risico's, geïdentificeerd door het management, en de risicobeheerprocessen binnen de volledige organisatie controleren*
- *zekerheid bieden inzake het beheer van de risico's*
- *actieve ondersteuning en betrokkenheid bieden in het risicobeheerproces*
- *risico-identificatie-/inschatting makkelijker maken en het personeel opleiden op het vlak van risicobeheer en interne controle*
- *coördineren van de risicorapportering aan de Raad, de auditcommissie, enz*

Bij het bepalen van de meest geschikte rol voor een bepaalde organisatie dient Interne Audit ervoor te zorgen dat de professionele vereisten voor onafhankelijkheid en objectiviteit niet geschonden worden.



8.6 Middelen en implementatie

De middelen nodig om het risicobeheerbeleid van een organisatie in praktijk te brengen, dienen duidelijk te worden vastgesteld op elk managementniveau en binnen elke business unit.

Naast de eventuele andere operationele functies die ze kunnen hebben, dienen degenen die betrokken zijn bij risicobeheer hun rol bij het coördineren van bij het risicobeheer/strategie duidelijk omschreven te hebben. Diezelfde duidelijke omschrijving is eveneens vereist voor degenen die betrokken zijn bij de audit en revisie van de interne controles en het bevorderen van het risicobeheerproces.

Het risicobeheer dient in de organisatie verankerd te zijn door middel van de strategie- en budgetprocessen. Er dient aandacht aan te worden besteed tijdens introductiecurricula en alle andere opleidingen en vormingen, alsook binnen de operationele processen bijv. product-/dienstenontwikkelingsprojecten.

9. Toezicht en revisie van het risicobeheerproces.

Een doeltreffend risicobeheer vereist een rapporterings- en revisiestructuur om te garanderen dat de risico's doeltreffend geïdentificeerd en ingeschat worden en dat de passende controlemaatregelen en respons zijn aangebracht. Het beleid dient geregeld

onderworpen te worden aan audits en ook de naleving van de normen dient op regelmatige tijdstippen te worden getoetst, om mogelijkheden voor verbetering te identificeren. Daarbij mag niet uit het oog worden verloren dat organisaties dynamisch zijn en in dynamische omgevingen werkzaam zijn. Wijzigingen in de organisatie en in de omgeving waarin ze werkzaam is, dienen te worden geïdentificeerd en waar nodig dienen de systemen te worden aangepast.

Het toezichtproces dient de garantie te bieden dat de activiteiten van de organisatie op passende wijze worden gecontroleerd en dat de procedures begrepen zijn en worden nageleefd. Wijzigingen in de organisatie en in de omgeving waarin ze werkzaam is, dienen te worden geïdentificeerd en waar nodig dienen de systemen te worden aangepast.

Elk toezicht- en revisieproces dient eveneens vast te stellen of:

- *de toegepaste maatregelen het verwachte resultaat opleveren*
- *de toegepaste procedures en de informatie verzameld voor de beoordeling geschikt waren*
- *een grondiger kennis geholpen zou hebben om betere beslissingen te nemen en welke lessen eruit kunnen worden getrokken voor toekomstige beoordelingen en beheer van risico's*



10. Bijlage

Technieken voor risico-identificatie - voorbeelden

- *brainstorming*
- *vragenlijsten*
- *bedrijfsstudies die elk bedrijfsproces afzonderlijk bekijken en zowel de interne processen als de externe factoren beschrijven die een invloed kunnen hebben op die processen*
- *benchmarking*
- *scenarioanalyse*
- *workshops over risicobeoordeling*
- *incidentonderzoek*
- *audit en inspectie*
- *HAZOP-studies (Hazard & Operability)*

Methoden en technieken voor risicoanalyse - voorbeelden

Positief risico

- *marktonderzoek*
- *prospectie*
- *testmarketing*
- *onderzoek en ontwikkeling*
- *bedrijfsimpactanalyse*

Beide

- *Dependency Modelling*
- *SWOT-analyse (Strengths, Weaknesses, Opportunities, Threats)*
- *gebeurtenissenboomanalyse (Event Tree Analysis of ETA)*
- *bedrijfscontinuïteitsplanning*
- *BPEST-analyse (Business, Political, Economic, Social, Technological)*
- *Real Option Modelling*
- *besluitvorming onder omstandigheden van risico en onzekerheid*
- *statistische gevolgtrekking*
- *maatstaven van centrale tendens en spreiding*
- *PESTLE (Political Economic Social Technical Legal Environmental)*

Negatief risico

- *dreiging-analyse*
- *foutenboomanalyse (Fault Tree Analysis of FTA)*
- *FMEA (Failure Mode & Effect Analysis)*



AGERS - Asociación Española de Gerencia de Riesgos y Seguros
Príncipe de Vergara, 86 - 1ª Esc., 2º Izda.- 28006 Madrid - SPAIN
Tel: + 34 91 562 84 25 – Fax: + 34 91 590 07 80 – Email: gerencia@agers.es – www.agers.es



AIRMIC - The association of Insurance and Risk Managers
Lloyd's Avenue, 6 – London EC3N3AX - UK
Tel: + 44 207 480 76 10 – Fax: + 44 207 702 37 52 – Email: enquiries@airmic.co.uk – www.airmic.com



AMRAE - Association pour le Management des Risques et des Assurances de l'Entreprise
Avenue Franklin Roosevelt, 9-11 – 75008 Paris - FRANCE
Tel: + 33 1 42 89 33 16 – Fax: + 33 1 42 89 33 14 – Email: amrae@amrae.fr – www.amrae.fr



ANRA - Associazione Nazionale dei Risk Manager e Responsabili Assicurazioni Aziendali
Via del Gonfalone 3, I-20123 Milano - ITALY
Tel: + 39 02 58 10 33 00 – Fax: + 39 02 58 10 32 33 – Email: anra@betam.it – www.anra.it



APOGERIS - Associação Portuguesa de Gestão de Riscos e Seguros
Avenida da Boavista, 1245, 3a Esq. – 4100-130 Porto – PORTUGAL
Tel: + 351 22 608 24 62 – Fax: + 351 22 608 24 73 – E-mail: anfernandes@sonae.pt – www.apogeris.pt



ASPAR CR - Association of Insurance and Risk Management of the Czech Republic o.s.
Nad Ohradou 7 – 13000 Praha 3 – Tel: + 420 602 384 256 – Email: asparcr@volny.cz



BELRIM - Belgian Risk Management Association
Rue Gatti de Gamond, 254 – 1180 Bruxelles - BELGIUM
Tel: + 32 2 389 23 95 – Fax: + 32 2 389 22 72 – Email: info@belrim.com – www.belrim.com



bfV - Bundesverband firmenverbundener Versicherungsvermittler und -Gesellschaften e.V.
c/o Mr Hans-Otto GEIGER – Postfach 1916 – D-67209 Frankenthal – GERMANY
Tel: + 49 6233 86 2507 - Fax: + 49 6233 86 2507 - Email: hans-otto.geiger@ksb.com – www.bfv-fvv.de



BRIMA - Bulgarian Risk Management Association
101, Tzarigradsko chaussee, floor 4 – Sofia 1113 – BULGARIA
Tel: + 359 878 100292 – Fax: + 359 2 971 0702 – Email: office@brima.biz – www.brima.biz



DARIM - DI's Risk Management Forening
DK-1787 Copenhagen – DENMARK
Tel: + 45 33 77 33 77 – Fax: + 45 33 77 33 00 – Email: darim@di.dk – www.di.dk



DVS - Deutscher Versicherungs-Schutzverband e.V.
Breite Strasse 98 - D 53111 Bonn - GERMANY
Tel: + 49 228 98 22 30 - Fax: + 49 228 63 16 51- Email: dvs@dvs-schutzverband.de – www.dvs-schutzverband.de



FINNRIMA - Finnish Risk Management Association
Talvikkitie 40 A 33, 01300 Vantaa – FINLAND
Tel: + 358 9 5607 5361 – Fax: + 358 9 5607 5365 – Email: srhy@hennax.fi – www.srhy.fi



NARIM - Nederlandse Associatie van Risk en Insurance Managers
P.O. Box 65707 - 2506 EA Den Haag – THE NETHERLANDS
Tel: + 31 70 345 7426 – Fax: + 31 70 427 3263 – Email: ielsdewild@imfo.nl – www.narim.com



POLRISK - Polish Risk Management Association
ul. Rzymowskiego 30 lok. 424 - 02-697 Warszawa - POLAND
Tel: + 48 22 331 8121 – Fax: + 48 22 331 81 22 – Email: info@polrisk.pl – www.polrisk.pl



RUSRISK - Russian Risk Management Society
Address Expert Institute, Staraya Ploshchad 10/4, Moscow, 103070 – RUSSIA
Tel: + 7 495 231 53 56 - Fax: + 7 495 231 53 56 - Email: info@rrms.ru – www.rrms.ru



SIRM - Swiss Association of Insurance and Risk Managers
Gutenbergstrasse 1, Postfach 5464, CH-3001 Bern - SWITZERLAND
Tel: + 41 31 388 87 89 – Fax: + 41 31 388 87 88 – Email: info@sirm.ch – www.sirm.ch

SWERMA - Swedish Risk Management Association
Gränsvägen 15 - SE-135 47 Tyresö - SWEDEN
Tel: + 468 742 13 07 - Fax: + 468 798 83 11- E-mail: info@swerma.se – www.swerma.se

ALARM - The National Forum for Risk Management in the Public Sector
Queens Drive, Exmouth - Devon, EX8 2AY
Tel: + 44 1395 223399 - Fax: + 44 1395 223304 - Email: admin@alarm.uk.com - www.alarm-uk.com



IRM - The Institute of Risk Management
6 Lloyd's Avenue - London EC3N 3AX
Tel: + 44 20 7709 9808 - Facsimile + 44 20 7709 0716 - Email: enquiries@theirm.org - www.theirm.org