BEST PRACTICE

Risicomanagement

op basis van M_o_R® en NEN/ISO 31000

Management Guide

Douwe Brolsma
Mark Kouwenhoven

Best Practice User Group NL
Incorporating PRINCE User Group

Van Haren PUBLISHING

Risicomanagement op basis van M_o_R®
en NEN/ISO 31000 – Management Guide

Andere uitgaven bij Van Haren Publishing

Van Haren Publishing (VHP) is gespecialiseerd in uitgaven over Best Practices, methodes en standaarden op het gebied van de volgende domeinen:

- IT en IT-management;
- Enterprise-architectuur;
- Projectmanagement, en:
- Businessmanagement.

Deze uitgaven zijn beschikbaar in meerdere talen en maken deel uit van toonaangevende series, zoals *Best Practice, The Open Group series, Project management* en *PM series.*

Op de website van Van Haren Publishing is in de **Knowledge Base** een groot aanbod te vinden van whitepapers, templates, gratis e-books, docentenmateriaal etc. Ga naar www.vanharen.net.

Van Haren Publishing is tevens de uitgever voor toonaangevende instellingen en bedrijven, onder andere: Agile Consortium, ASL BiSL Foundation, CA, Centre Henri Tudor, Gaming Works, IACCM, IAOP, IPMA-NL, ITSqc, NAF, Ngi, PMI-NL, PON, The Open Group, The SOX Institute.

Onderwerpen per domein zijn:

IT en IT-management
ABC of ICT™
ASL®
CATS CM®
CMMI®
COBIT
e-CF
ISO 17799
ISO/IEC 27001/27002
ISO/IEC 20000
ISPL
IT Service CMM
ITIL®
MOF
MSF
SABSA

Architecture (Enterprise en IT)
ArchiMate®
GEA®
Novius Architectuur Methode
TOGAF®

Business Management
BiSL®
EFQM
eSCM
IACCM
ISA-95
ISO 9000/9001
OPBOK
SAP
SixSigma
SOX
SqEME®

Project-, Programma- en Risicomanagement
A4-Projectmanagement
ICB / NCB
ISO 21500
MINCE®
M_o_R®
MSP®
P3O®
PMBOK® Guide
PRINCE2®

Risicomanagement
op basis van M_o_R®
en NEN/ISO 31000

Management Guide

Douwe Brolsma en Mark Kouwenhoven

Van Haren PUBLISHING

Colofon

Titel:	Risicomanagement op basis van M_o_R® en NEN/ISO 31000 – Management Guide
Auteurs:	Douwe Brolsma Mark Kouwenhoven
Reviewer:	Hans M. Schneider (voorzitter Best Practice User Group NL)
Tekstredactie:	Timon Meynen (Meynen Tekstadvies)
Illustraties:	Ramon Verberne (nThen! BV)
Uitgever:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN Boek:	978 90 8753 656 5
ISBN eBoek:	978 90 8753 959 7
Druk:	Eerste druk, eerste oplage, januari 2012 Eerste druk, tweede oplage, maart 2014
DTP-productie:	CO2 Premedia, Amersfoort – NL

Voorwoord

'Wie een Risicoloos bestaan wil leiden, komt tot niets'
(oud-minister Johan Remkes, 27 augustus 2010, interview Radio 1)

Zo gewoon als de termen 'Risico's' en 'Risicomanagement' ons in de oren klinken, zo onbekend, complex en vaak onbegrepen is de wereld die erachter schuilgaat. Net voor de eeuwwisseling vond er een verandering in het denken over risico's plaats. Waar daarvoor Risico's altijd refereerde aan negatieve gebeurtenissen die je succes dwarsbomen, ging men rond die tijd risico's meer zien als onbekende gebeurtenissen die invloed hebben op je succes, en dat kunnen dan ook positieve gebeurtenissen zijn - oftewel 'mogelijkheden' of 'Kansen'. Jammer genoeg blijven veel mensen bij de term 'Risicomanagement' alleen denken aan negatieve zaken.

Een organisatie die zijn Risicomanagement volwassen heeft ingericht, blinkt uit in het besef dat Risico's niet uitgesloten kunnen worden. In iedere beslissing schuilt een mate van onzekerheid hoe deze zal uitpakken. De medewerkers in een organisatie met een Risicobewuste cultuur zijn zich hiervan bewust en wegen Bedreigingen af tegen Kansen voordat beslissingen genomen worden. Ze accepteren dat het soms ook mis kan gaan, proberen hier wat van te leren en gaan door zonder elkaar te veroordelen.

Er is een aantal zogenaamde frameworks of richtlijnen voor ERM (Enterprise Risk Management) die integraal toepasbaar zijn en organisatiebreed werken: de NEN/ISO 31000-norm voor Risicomanagement, COSO – integrated framework en M_o_R® (Management of Risk). In dit boek komen deze alle drie aan de orde, maar de meeste aandacht gaat uit naar M_o_R omdat dit framework de meest praktische handvatten geeft en in lijn is met NEN/ISO 31000.

Het boek is bedoeld om mensen en organisaties te helpen succesvoller te zijn door het nemen van betere besluiten als gevolg van het toepassen van Risicomanagement. Daarbij wordt alles bekeken in de Nederlandse context, die vaak een internationaal tintje heeft. We hopen dat dit een aanzet kan zijn tot Risicobewuster en proactievere samenwerking in organisaties.

December 2011, de auteurs

Inhoudsopgave

Leeswijzer

Dit boek gaat over het beheersen van Risico's in organisaties en projecten. Daarbij wordt veel aandacht besteed aan de belangrijkste richtlijnen op het gebied van Risicomanagement. Omdat het framework M_o_R de meest praktische aanpak biedt, hanteren we deze als uitgangspunt in de hoofdstukken 2 t/m 5. Dit boek sluit aan op M_o_R 2010 Edition, zoals beschreven in *Management of Risk: Guidance for Practitioners - 2010 Edition*. Daarnaast wordt regelmatig verwezen naar de *NEN/ISO 31000 Risicomanagement - principes en richtlijnen* (NEN/ISO 31000:2009, IDT), aangezien M_o_R hier nauw bij aansluit. Tevens wordt in bijlage D aandacht besteed aan 'COSO - integrated framework', BASEL I, II, III, de code-Tabaksblat en de Nederlandse standaard voor Risicomanagement in de bouw - RISMAN.

Hoofdstuk 1 introduceert de belangrijkste Risicomanagementtermen en legt uit wat Risicomanagement is, waarom het belangrijk is voor organisaties, en waar en door wie het wordt toegepast. Bijlage D over de belangrijkste (inter)nationale richtlijnen op het gebied van Risicomanagement kan hierbij als extra informatie gelezen worden.

Hoofdstuk 2 geeft uitleg over het M_o_R-framework: de principes van Governance en de toepassing van de principes op vier perspectieven: het strategisch, programma-, project- en operationeel perspectief.

Hoofdstuk 3 gaat dieper in op de Risicomanagementaanpak en de bijbehorende documenten.

Hoofdstuk 4 geeft een overzicht van de processtappen van M_o_R, wanneer het proces wordt toegepast en de communicatie en de technieken die eventueel gebruikt kunnen worden om de verschillende stappen in het Risicomanagementproces te ondersteunen.

Hoofdstuk 5 behandelt het verankeren en reviewen van Risicomanagement in de organisatie, implementatie van Risicomanagement, omgang met weerstand en wat daarbij komt kijken.

Bijlage A geeft concrete voorbeelden en extra informatie over de verschillende technieken die de processtappen beschreven in hoofdstuk 4 ondersteunen.

Bijlage B - Gezondheidscheck en Volwassenheidsmodel voor Risicomanagement kan samen met hoofdstuk 5 bestudeerd worden.

Bijlage C - De Risicospecialismen geven extra informatie over 8 specialisaties op het gebied van Risicomanagement.

Bijlage D - Andere Risicogerelateerde richtlijnen geef een korte beschrijving van andere richtlijnen in de wereld en hoe ze zich verhouden tot M_o_R. Het kan gelezen worden als extra informatie bij hoofdstuk 1.

In ieder hoofdstuk zijn kaders opgenomen met praktijkvoorbeelden en tips over de toepassing van Risicomanagement.

Het M_o_R Foundation exam - Deze Management Guide kan ook worden gebruikt ter voorbereiding op het M_o_R Foundation-examen van APMG. Alle benodigde kennis voor het examen is in dit boek te vinden. De voorbeelden maken geen deel uit van de stof die getoetst wordt in het M_o_R Foundation-examen. Ook de vergelijking van M_o_R met andere richtlijnen, zoals COSO, BASEL, NEN/ISO 31000 en code-Tabaksblat, is geen onderdeel van de eindtermen voor het M_o_R-examen van APMG.

Dit boek biedt een brede kijk op Risicomanagement, beschouwd in relatie tot een Nederlandse context, met achtergrondinformatie, praktijkvoorbeelden en tips voor succesvolle toepassing.

De typische Risicomanagementtermen beginnen met een hoofdletter om ze extra te benadrukken.

HOOFDSTUK 1

Inleiding en achtergrond

In het licht van de recente wereldwijde ontwikkelingen op het gebied van economische en financiële regelgeving is er duidelijk een groeiende belangstelling voor richtlijnen die organisaties helpen op een volwassen manier met Risico's om te gaan. Het nadeel van de meeste methoden is dat ze voortkomen uit de financiële wereld en vooral gericht zijn op beheersing van (financiële) Risico's, gezien vanuit het strategisch perspectief.

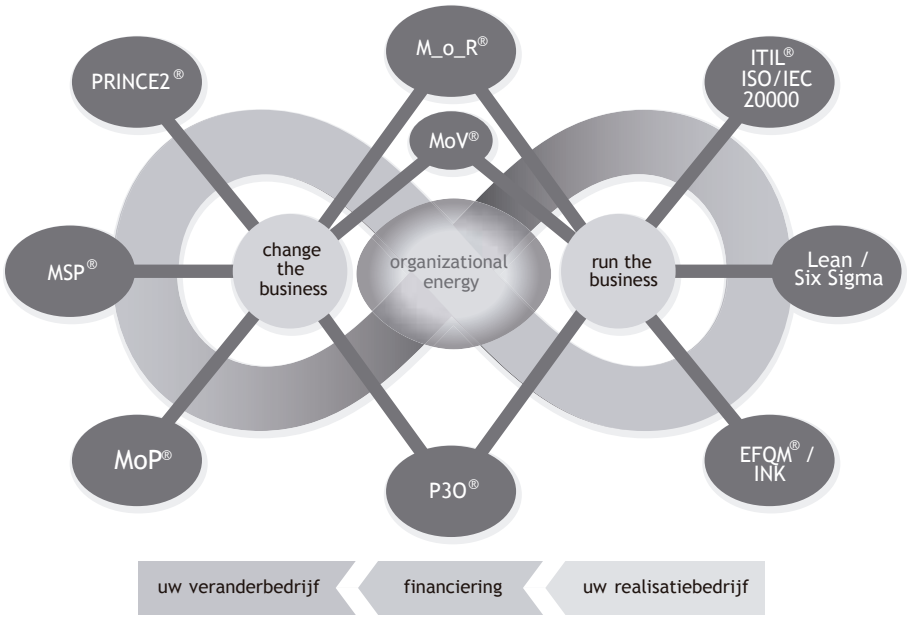
Hoewel organisaties ook op operationeel niveau actief Risico's managen wordt dit werk vaak niet als zodanig herkend of in een breder kader aangepakt. Zo hebben veel organisaties processen en procedures die erop toezien dat de bedrijfscontinuïteit wordt gewaarborgd bij kritieke incidenten en worden alle organisaties geacht te voldoen aan wet- en regelgeving omtrent Gezondheid en Veiligheid. Drijfveren daarbij zijn kwaliteit, service, continuïteit en klantgerichtheid. Kortom we doen al veel meer aan Risicomanagement dan we beseffen.

Het M_o_R-framework (Management of Risk framework - zie figuur 1.2) is ontwikkeld op basis van best practices om te dienen als beheersingsinstrument (*control*) voor behoorlijk bestuur (Corporate Governance). Naast Risicomanagement bestaat Corporate Governance uit financieel management, operationeel management en naleving (*compliance*)). Risicomanagement staat aan de basis van verantwoorde besluitvorming in organisaties en is daarbij ook volledig geïntegreerd in de overige best-practiceframeworks en methoden van AXELOS Limited (zie in figuur 1.1 hoe de frameworks en methoden zich tot elkaar verhouden).

M_o_R is integraal toepasbaar en specifiek uitgewerkt voor vier perspectieven in een organisatie, namelijk:

– het strategisch perspectief, waarin het over beslissingen over de langetermijndoelen van een organisatie gaat; zie ook **MoP**® Management of Portfolio's;
– het programma- en het projectperspectief, waarin het gaat over middellangetermijndoelen en de besluitvorming daaromtrent; zie ook **MSP**® - Managing Successful Programmes en **PRINCE2**® voor projectmanagement;
– het operationele perspectief, waarin het gaat over de kortetermijndoelen, de dagelijkse gang van zaken (Business as Usual) en de besluitvorming omtrent bedrijfscontinuïteit; zie ook **ITIL**® voor de operationele werkzaamheden van IT-servicemanagement.

Uiteraard is het van belang dat beslissingen op operationeel niveau de besluitvorming op de andere niveaus ondersteunen (en omgekeerd misschien soms ook wel).



Figuur 1.1 Best-practicemethoden in perspectief

Centraal staat de 'energie' van de organisatie: door het mobiliseren van energie is een organisatie in staat om het dagelijks werk in het bedrijf (*run the business*) te combineren met de voorbereiding op de toekomst door het veranderen van het

bedrijf (*change the business*). Dit wordt methodisch ondersteund door een familie van onderling verbonden best-practiceframeworks en methoden die elk met een eigen nadruk een aanvulling vormen op het gezond verstand, zie fig. 1.1:

- **M_o_R®** (Management of Risk) voor Risicomanagement.
- **PRINCE2®** voor projectmanagement.
- **MSP®** - Managing Successful Programmes voor programmamanagement.
- **MoP®** Management of Portfolio's voor portfoliomanagement voor het strategisch niveau.
- **P3O®** - Portfolio, Program en Project Offices voor het inrichten van ondersteuning in de organisatie.
- **MoV®** - Management of Value voor het bepalen en managen van waarden in organisaties.
- **ITIL®** en **ISO/IEC 20000** voor de werkzaamheden in het kader van IT-servicemanagement.

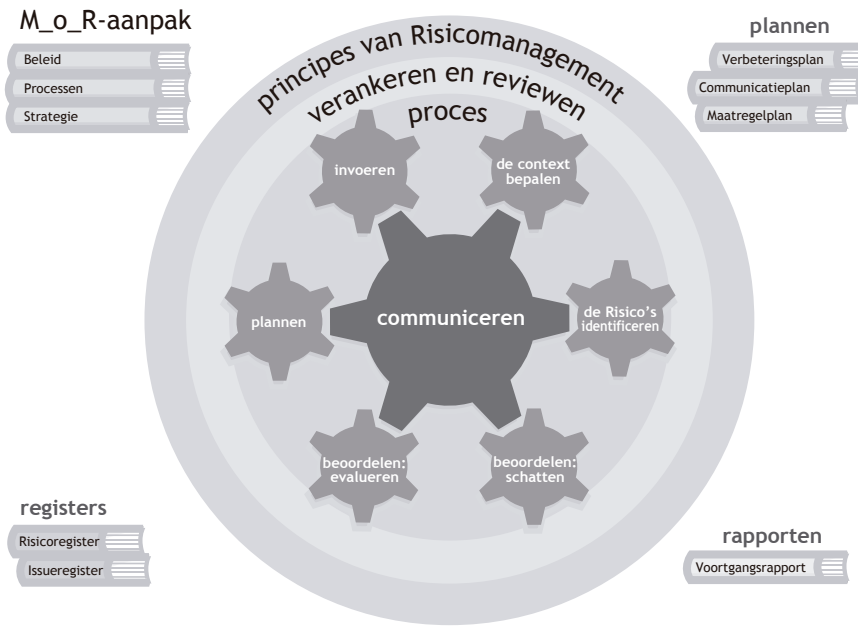
1.1 Doel van het framework Management of Risk

Management of Risk, afgekort als M_o_R, beoogt een hulpmiddel te zijn voor personen en organisaties om succesvoller te zijn. Het bewuster en explicieter omgaan met Risico's verbetert en versnelt besluitvorming op de weg naar het bereiken van je doel(en).

M_o_R biedt een generieke richtlijn die geschikt is voor het identificeren, wegen en beheersen van Risico's in alle soorten organisaties. Dit framework heeft niet alleen aandacht voor het strategisch niveau, maar ook voor de operationele bedrijfsvoering (BAU, Business As Usual) en de veranderorganisatie. Hierbij worden een aantal rollen benoemd die organisaties helpen beter te communiceren ter ondersteuning van het managen en nemen van Risico's.

Het M_o_R-framework is gebaseerd op vier kernconcepten, zie fig. 1.2.

1. **De M_o_R-principes**. Deze principes zijn afgeleid van de principes van Corporate Governance. In het kader van Corporate Governance wordt Risicomanagement genoemd als een van de interne beheersinstrumenten (*controls*) van iedere organisatie, naast financiële en operationele beheersinstrumenten en naleving.



Figuur 1.2 Het M_o_R-framework, gebaseerd op M_o_R 2010 Edition

Hoofdstuk 2 gaat nader in op de principes van Risicomanagement en hierin wordt ook een voorbeeld gegeven hoe de principes inhoud krijgen op strategisch, programma-, project- en operationeel niveau.

2. **De M_o_R-aanpak**. De principes moeten voor de specifieke organisatie worden aangepast en door de gehele organisatie worden toegepast. Hiervoor is een aantal managementdocumenten ontworpen, namelijk:
   a. Een algemene beleidslijn.
   b. Een procesbeschrijving van de Risicomanagementactiviteiten.
   c. Een strategisch document waarin het beleid is uitgewerkt voor een specifieke activiteit.
   d. Plannen voor het bewaken van de invoering van Risicomanagement in de organisatie en voor de uitvoering en bewaking van Risicobeheersmaatregelen. Daarnaast wordt ook het Risicocommunicatieplan (*Risk Communication Plan*) nog apart genoemd.

e. Registers, zoals het Risico- en Issueregister moeten ervoor zorgen dat Risico's en Issues worden geïdentificeerd en vastgelegd.
f. Risicorapportages die de stand van zaken van Risicomanagement rond een activiteit weergeven.

Hoofdstuk 3 zal nader ingaan op deze Risicomanagementdocumenten.

3. **De M_o_R-processen**. Alle activiteiten rondom het managen van Risico's zijn samen te vatten in een procesbeschrijving. M_o_R gaat uit van een model met vier hoofdstappen. De eerste twee stappen bestaan ieder ook weer uit twee substappen, in totaal worden er 6 stappen benoemd.
   1. Identificeren: De context bepalen.
   2. Identificeren: De Risico's identificeren.
   3. Beoordelen: Schatten.
   4. Beoordelen: Evalueren.
   5. Plannen.
   6. Invoeren (van beheersmaatregelen).

   Bij al deze stappen is communicatie van cruciaal belang, aangezien Risico's nooit statisch zijn en alle betrokken partijen goed op de hoogte gehouden moeten worden om aan hun verantwoordelijkheden te kunnen voldoen.

   In hoofdstuk 4 worden de stappen behandeld, inclusief de meest gebruikte technieken die het werk kunnen ondersteunen en de resultaten die de processtappen opleveren.

4. **M_o_R verankeren en reviewen**. Uitgangspunt van een volwassen organisatie is dat Risicomanagement consistent wordt toegepast en voortdurend wordt verbeterd. Het is van belang dat de organisatie periodiek haar Risicomanagementpraktijken tegen het licht houdt om te zorgen dat ze efficiënt en effectief blijven. Op deze manier is er sprake van continue verbetering en een stijging van het Volwassenheidsniveau van een organisatie.

   Hoofdstuk 5 is gewijd aan dit deel van het framework.

1.2 Wat is een Risico?

Uit spreekwoorden blijkt hoezeer we al gewend zijn aan het managen van Risico's. Bijvoorbeeld: 'Een gewaarschuwd mens telt voor twee'. Maar ook bekende uitspraken laten zien hoezeer onzekerheid een deel van het leven is. Bijvoorbeeld de wet van Murphey: 'Als er iets mis kan gaan, dan gaat het mis'.

M_o_R geeft voor 'Risico' de volgende definitie:

Definitie
'Een Risico is een onzekere gebeurtenis of reeks gebeurtenissen die, als die zou plaatsvinden, Gevolg zou hebben op het bereiken van doelstellingen.'

Een Risico bestaat uit een combinatie van de Waarschijnlijkheid (*probability*) dat een Bedreiging of Kans[1] plaatsvindt en de gevolgen (Gevolg) ervan, ook wel Impact genoemd, op de doelstellingen.

Dit Gevolg kan zowel positief als negatief van aard zijn. Een onzekere gebeurtenis die een negatieve Impact zou kunnen hebben op doelstellingen of Benefits wordt een 'Bedreiging' (*threat*) genoemd, en een onzekere gebeurtenis die een gunstige Impact zou kunnen hebben op doelstellingen of Benefits een 'Kans' of 'mogelijkheid' (*opportunity*).

NEN/ISO 31000 noemt een Risico het Effect (positief en negatief) van onzekerheid op het behalen van doelstellingen, waarbij er een verwijzing is naar mogelijke *gebeurtenissen* en *gevolgen* en de bijbehorende *Waarschijnlijkheid* dat de gebeurtenis zich voordoet.

COSO beschrijft een Risico als een mogelijke gebeurtenis met een mogelijke negatieve Impact op een doelstelling. Gebeurtenissen met een positieve Impact zijn mogelijkheden. De beoordeling vindt plaats aan de hand van Waarschijnlijkheid en Impact.

1 Het woord 'Kans' kan zowel Waarschijnlijkheid van optreden als mogelijkheid betekenen. Om verwarring en misinterpretatie te voorkomen gebruiken we in dit boek zo consequent mogelijk het woord 'Waarschijnlijkheid' als uiting van onzekerheid (onzekere verwachting) en reserveren we de woorden 'Kans' en 'mogelijkheid' voor de uiting van een positief Gevolg (verwachting van een gunstig Gevolg).