Nederlandse norm

NEN-ISO 31000

(nl)

Risicomanagement - Principes en richtlijnen
(ISO 31000:2009,IDT)

Risk management - Principles and guidelines
(ISO 31000:2009,IDT)

ICS 03.100.01
december 2009

Dit document bevat de vertaling in het Nederlands van de internationale norm ISO 31000:2009. De internationale norm ISO 31000:2009 heeft de status van Nederlandse norm.

Normcommissie 400179 "Risicomanagement"

NEN

©2009 Nederlands Normalisatie-instituut
Postbus 5059, 2600 GB Delft
Telefoon (015) 2 690 390, Fax (015) 2 690 190

A.1 Inhoud

Voorwoord

ISO (International Organization for Standardization) is een wereldwijde federatie van nationale normalisatie-instituten (de ISO-leden). Het voorbereidingswerk voor internationale normen wordt doorgaans uitgevoerd door de technische commissies van ISO. Elk lid dat interesse heeft in een onderwerp waarvoor een technische commissie is samengesteld, heeft recht op vertegenwoordiging in deze commissie. Internationale organisaties, zowel overheidsinstanties als niet-gouvernementele organisaties, nemen in samenwerking met ISO ook deel aan deze werkzaamheden. ISO werkt nauw samen met de International Electrotechnical Commission (IEC) inzake alle elektrotechnische normalisatie.

Internationale normen worden opgesteld overeenkomstig de voorschriften die in de ISO/IEC-richtlijnen deel 2 zijn opgenomen.

De voornaamste taak van de technische commissies is de voorbereiding van internationale normen. Ontwerpversies van internationale normen die zijn aangenomen door de technische commissies, worden ter stemming voorgelegd aan de leden. Publicatie als internationale norm vereist goedkeuring van ten minste 75 % van de stemmen die zijn uitgebracht door deelnemende leden.

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp kunnen zijn van patentrechten. ISO is niet verantwoordelijk voor identificatie van dergelijke patentrechten.

ISO 31000 werd opgesteld door de werkgroep voor risicomanagement van de ISO Technical Management Board.

Inleiding

Ongeacht type en omvang van de organisatie, wordt elke organisatie geconfronteerd met interne en externe factoren en invloeden die ertoe leiden dat het onzeker is of en wanneer zij haar doelstellingen zal behalen. Het effect dat deze onzekerheid heeft op de doelstellingen van de organisatie, is ‘risico’.

Alle activiteiten van een organisatie zijn onderhevig aan bepaalde risico’s. Organisaties managen risico’s door deze te identificeren en te analyseren, en vervolgens te beoordelen of het risico behoort te worden aangepast door middel van risicobehandeling, zodat aan de risicocriteria van de organisatie wordt voldaan. Gedurende dit proces communiceren en overleggen de organisaties met belanghebbenden en monitoren en beoordelen ze het risico en de beheersmaatregelen die het risico aanpassen om ervoor te zorgen dat geen verdere risicobehandeling nodig is. Dit systematische en logische proces wordt in deze internationale norm in detail beschreven.

Hoewel elke organisatie tot op zekere hoogte risico’s managet, wordt in deze internationale norm een aantal principes beschreven waaraan moet worden voldaan wil er sprake zijn van doeltreffend risicomanagement. In deze internationale norm wordt aanbevolen dat een organisatie een kader ontwikkelt, implementeert en continu verbetert dat tot doel heeft het proces van risicomanagement te integreren in het algemene bestuur (‘governance’), de strategie en planning, het management, de rapportageprocessen, beleid(slijnen), waarden en cultuur van de organisatie.

Risicomanagement kan zowel worden toegepast op een organisatie als geheel, op al haar afdelingen en niveaus, op elk moment, als op specifieke functies, projecten en activiteiten.

Hoewel de praktijk van risicomanagement zich in de loop der tijd in vele sectoren heeft ontwikkeld om aan allerlei behoeften te voldoen, kan de implementatie van consistente processen in een breed kader ertoe bijdragen dat risico’s doeltreffend, doelmatig en op een coherente wijze worden gemanaged in alle lagen van de organisatie. De generieke benadering die in deze internationale norm wordt beschreven, omvat principes en richtlijnen voor het management van alle vormen van risico’s op een systematische, transparante en betrouwbare wijze, binnen elke reikwijdte en context.

Elke specifieke sector of toepassing van risicomanagement wordt gekenmerkt door eigen behoeften, publiek, inzichten en criteria. Een belangrijk kenmerk van deze internationale norm is dan ook de opname van het ‘vaststellen van de context’ als activiteit aan het begin van het generieke risicomanagementproces. Bij het vaststellen van de context worden de doelstellingen van de organisatie beschreven, de omgeving waarin de

organisatie deze doelstellingen wil behalen, wie de belanghebbenden zijn en de diversiteit aan risicocriteria. Al deze factoren helpen de aard en complexiteit van de risico's vast te stellen en te beoordelen.

De relatie tussen de principes voor het management van risico's, het kader waarin dit plaatsvindt en het risicomanagementproces zoals dat in deze internationale norm wordt beschreven, is weergegeven in figuur 1.

Als risicomanagement wordt geïmplementeerd en onderhouden overeenkomstig deze internationale norm, zal het een organisatie in staat stellen, bijvoorbeeld:

— de kans te vergroten dat zij haar doelstellingen behaalt;

— proactief management te stimuleren;

— bewust te zijn van de noodzaak tot het identificeren en behandelen van risico's in alle lagen van de organisatie;

— identificatie van kansen en bedreigingen te verbeteren;

— te voldoen aan relevante eisen uit wet- en regelgeving en internationale normen;

— verplichte en vrijwillige vormen van rapportage te verbeteren;

— bestuur ('governance') te verbeteren;

— voor meer vertrouwen onder haar belanghebbenden te zorgen;

— een betrouwbare basis te leggen voor besluitvorming en planning;

— beheersmaatregelen te verbeteren;

— middelen voor risicobehandeling doeltreffend toe te wijzen en te benutten;

— de operationele doeltreffendheid en doelmatigheid te verbeteren;

— de arboprestaties te verbeteren, evenals de bescherming van het milieu;

— preventie van verliezen en incidentmanagement te verbeteren;

— verliezen te minimaliseren;

— leerprocessen in de organisatie te verbeteren; en

— het herstelvermogen van de organisatie te verbeteren.

Deze internationale norm beoogt te voldoen aan de behoeften van diverse belanghebbenden, waaronder:

a) personen die verantwoordelijk zijn voor de ontwikkeling van risicomanagementbeleid binnen de organisatie;

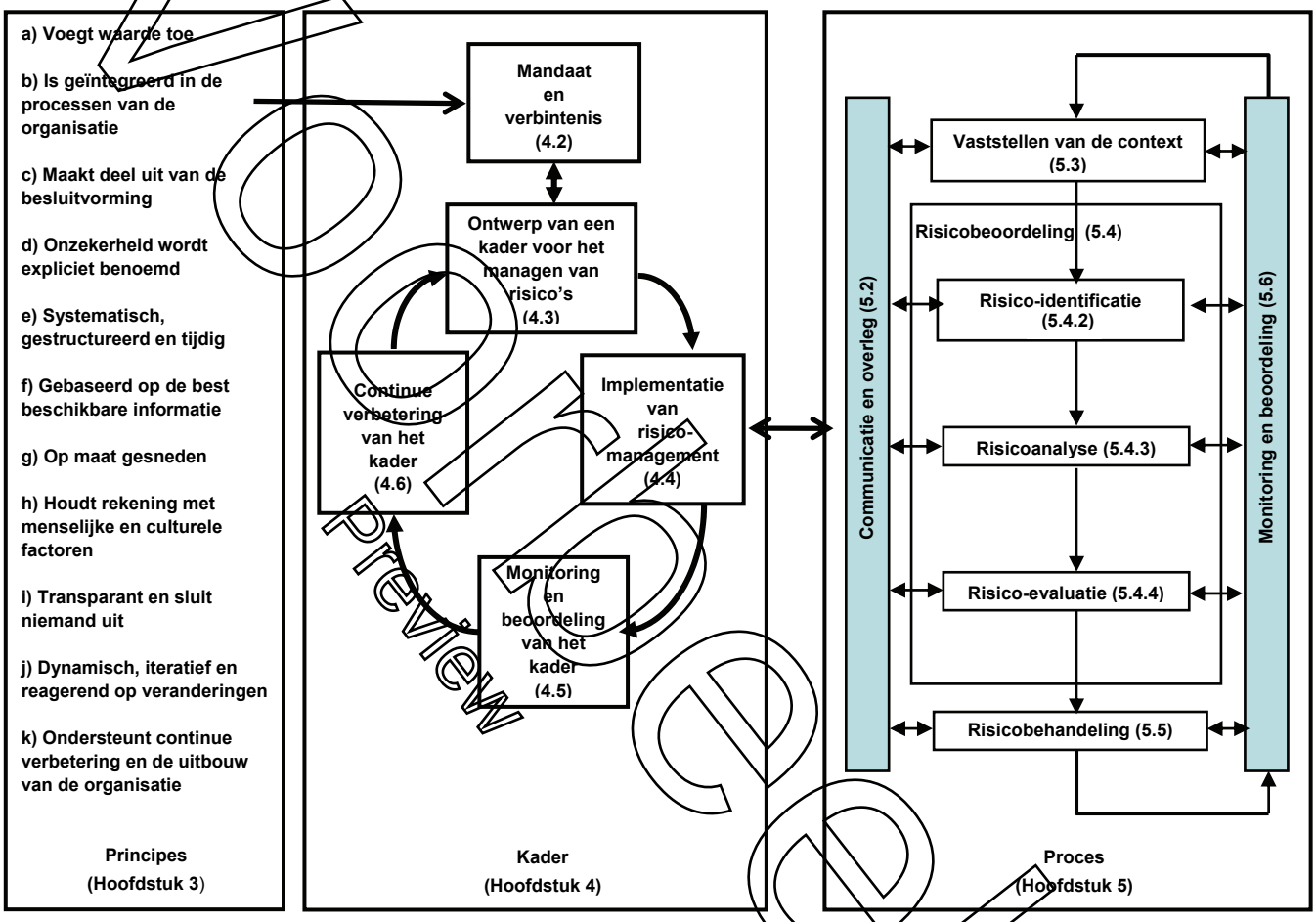
b) personen die verantwoordelijk zijn voor het doeltreffend managen van risico's binnen de organisatie als geheel, of binnen een bepaalde afdeling, bepaald project of bepaalde activiteit;

c) personen die moeten beoordelen in hoeverre een organisatie risico's doeltreffend managet; en

d) personen die normen, richtlijnen, procedures en praktijkcodes ontwikkelen waarin volledig of deels uiteen wordt gezet hoe risico's moeten worden gemanaged in de specifieke context van deze documenten.

In vele organisaties bevatten de huidige werkwijzen en beheersprocessen elementen van risicomanagement, en vele organisaties hebben al een formeel risicomanagementproces geïmplementeerd voor bepaalde typen risico's of voor bepaalde omstandigheden. In dergelijke gevallen kan een organisatie ervoor kiezen een kritische beoordeling van de bestaande werkwijzen en processen uit te voeren in het licht van deze internationale norm.

In deze internationale norm worden zowel de uitdrukkingen 'risicomanagement' als 'het managen van risico's' gebruikt. In algemene zin verwijst 'risicomanagement' naar de architectuur (principes, kader en proces) voor het doeltreffend managen van risico's, terwijl 'het managen van risico's' verwijst naar de toepassing van die architectuur op bepaalde risico's.



Figuur 1 — Relaties tussen de principes en kader voor en processen van risicomanagement

Risicomanagement – Principes en richtlijnen

1 Onderwerp en toepassingsgebied

Deze internationale norm bevat principes en algemene richtlijnen voor risicomanagement.

Deze internationale norm kan worden gebruikt door elke publieke, private of maatschappelijke onderneming, vereniging, groep of elk individu. Deze internationale norm is dan ook niet toegesneden op een specifieke bedrijfstak of sector.

OPMERKING Voor het gemak wordt elke gebruiker van deze internationale norm aangeduid met de algemene term 'organisatie'.

Deze internationale norm kan worden toegepast gedurende de gehele levenscyclus van een organisatie en op een breed scala aan activiteiten, zoals strategie- en besluitvorming, operationele bedrijfsactiviteiten, processen, functies, projecten, producten, diensten en bedrijfsmiddelen.

Deze internationale norm kan worden toegepast op elk type risico, ongeacht de aard, en ongeacht of het positieve dan wel negatieve gevolgen heeft.

Hoewel deze internationale norm generieke richtlijnen biedt, heeft de norm niet tot doel uniformiteit in risicomanagement tussen verschillende organisaties na te streven. Bij het ontwerp en de implementatie van plannen en kaders voor risicomanagement zal men rekening moeten houden met de wisselende behoeften van een specifieke organisatie, haar specifieke doelstellingen, context, structuur, operationele bedrijfsactiviteiten, processen, functies, projecten, producten, diensten of bedrijfsmiddelen en de specifieke werkwijzen die in die organisatie worden toegepast.

Deze internationale norm heeft tot doel risicomanagementprocessen in bestaande en toekomstige normen te harmoniseren. De norm biedt een gemeenschappelijke benadering ter ondersteuning van normen voor specifieke risico's en/of sectoren, en heeft niet tot doel deze normen te vervangen.

Deze internationale norm is niet bedoeld voor certificering.

2 Termen en definities

Voor de toepassing van deze norm gelden de volgende termen en definities.

2.1
risico
effect van onzekerheid op het behalen van doelstellingen

OPMERKING 1 Een effect is een afwijking ten opzichte van de verwachting – positief en/of negatief.

OPMERKING 2 Doelstellingen kunnen worden gekenmerkt door verschillende aspecten (bijvoorbeeld financiële, arbo- of milieudoelen) en kunnen betrekking hebben op verschillende niveaus (zoals strategisch, organisatiebreed, een project, product of proces).

OPMERKING 3 Een risico wordt vaak gekarakteriseerd door verwijzing naar mogelijke **gebeurtenissen** (2.17) en **gevolgen** (2.18), of een combinatie daarvan.

OPMERKING 4 Een risico wordt vaak uitgedrukt als een combinatie van de gevolgen van een gebeurtenis (met inbegrip van wijzigingen in omstandigheden) en de bijbehorende **waarschijnlijkheid** (2.19) dat de gebeurtenis zich voordoet.

OPMERKING 5 Onzekerheid is het geheel of gedeeltelijk ontbreken van informatie over, inzicht in of kennis van een gebeurtenis, de gevolgen daarvan of de waarschijnlijkheid dat deze zich voordoet.

[ISO Guide 73:2009, definitie 1.1]

2.2
risicomanagement
gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot **risico's** (2.1)

[ISO Guide 73:2009, definitie 2.1]

2.3
kader voor risicomanagement
geheel van componenten die de basis en organisatorische maatregelen bieden voor ontwerp, implementatie, **monitoring** (2.28), beoordeling en continue verbetering van **risicomanagement** (2.2) in alle lagen van de organisatie

OPMERKING 1 De basis omvat beleid, doelstellingen en mandaat voor en de verbintenis tot het managen van **risico's** (2.1).

OPMERKING 2 De organisatorische maatregelen omvatten plannen, relaties, verantwoordelijkheden, middelen, processen en activiteiten.

OPMERKING 3 Het kader voor risicomanagement is ingebed in de algemene strategische en operationele beleidslijnen en werkwijzen van de organisatie.

[ISO Guide 73:2009, definitie 2.1.1]

2.4
risicomanagementbeleid
verklaring van de algemene bedoelingen en richting van een organisatie met betrekking tot **risicomanagement** (2.2)

[ISO Guide 73:2009, definitie 2.1.2]

2.5
risicohouding
benadering van een organisatie bij de beoordeling en het uiteindelijk nastreven, behouden, nemen of vermijden van **risico's** (2.1)

[ISO Guide 73:2009, definitie 3.7.1.1]

2.6
risicomanagementplan
schema binnen het **kader voor risicomanagement** (2.3) waarin de benadering, de managementcomponenten en de middelen worden gespecificeerd die voor het management van **risico's** (2.1) worden aangewend

OPMERKING 1 Managementcomponenten omvatten doorgaans procedures, werkwijzen, toewijzing van verantwoordelijkheden, volgorde en tijdsplanning van activiteiten.

OPMERKING 2 Het risicomanagementplan kan worden toegepast op een bepaald product, proces en project, en op de gehele organisatie of een deel ervan.

[ISO Guide 73:2009, definitie 2.1.3]

2.7
risico-eigenaar
persoon of entiteit met de verantwoordelijkheid en bevoegdheid om het **risico** (2.1) te managen

[ISO Guide 73:2009, definitie 3.5.1.5]

2.8
risicomanagementproces
systematische toepassing van beleidslijnen, procedures en werkwijzen op de activiteiten met betrekking tot communicatie, overleg, vaststelling van de context, en het identificeren, analyseren, evalueren, behandelen, **monitoren** (2.28) en beoordelen van **risico's** (2.1)

[ISO Guide 73:2009, definitie 3.1]

2.9
vaststelling van de context
vaststelling van de externe en interne parameters waarmee rekening moet worden gehouden bij het managen van risico's en het vaststellen van de reikwijdte en de **risicocriteria** (2.22) voor het **risicomanagementbeleid** (2.4)

[ISO Guide 73:2009, definitie 3.3.1]

2.10
externe context
externe omgeving waarin de organisatie streeft naar het behalen van haar doelstellingen

OPMERKING De externe context kan het volgende omvatten:

— de culturele, maatschappelijke, politieke, wettelijke, regelgevende, financiële, technologische, economische, natuurlijke en concurrentieomgeving, op internationaal, nationaal, regionaal of lokaal niveau;

— belangrijke sturende factoren en trends die invloed hebben op de doelstellingen van de organisatie; en

— relaties met, en percepties en waarden van, externe **belanghebbenden** (2.13).

[ISO Guide 73:2009, definitie 3.3.1.1]

2.11
interne context
interne omgeving waarin de organisatie streeft naar het behalen van haar doelstellingen

OPMERKING De interne context kan het volgende omvatten:

— bestuur ('governance') en structuur van de organisatie, rollen en verantwoordelijkheden;

— beleid, doelstellingen, en de aanwezige strategieën om deze te behalen;

— het vermogen in termen van middelen en kennis (bijvoorbeeld kapitaal, tijd, personeel, processen, systemen en technologieën);

— informatiesystemen, informatiestromen en besluitvormingsprocessen (zowel formeel als informeel);

— relaties met, en percepties en waarden van, interne belanghebbenden;

— de cultuur van de organisatie;

— normen, richtlijnen en modellen die binnen de organisatie worden gehanteerd; en

— vorm en reikwijdte van contractuele verplichtingen.

[ISO Guide 73:2009, definitie 3.3.1.2]

2.12
communicatie en overleg
continue en iteratieve processen die een organisatie hanteert om informatie te leveren, uit te wisselen of te verkrijgen, en om een dialoog aan te gaan met **belanghebbenden** (2.13) die betrokken zijn bij het management van **risico's** (2.1)

OPMERKING 1 De informatie kan verband houden met de aanwezigheid, aard, vorm, **waarschijnlijkheid** (2.19), belangrijkheid, evaluatie, aanvaardbaarheid, behandeling of andere aspecten van (het management van) risico's [1)].

OPMERKING 2 Overleg is een tweerichtingsproces van onderbouwde communicatie tussen een organisatie en haar belanghebbenden over een bepaalde kwestie, voordat een besluit wordt genomen of een richting wordt bepaald met betrekking tot die kwestie. Overleg:

— is een proces dat effect heeft op de besluitvorming, eerder door invloed dan door macht; en

— levert een bijdrage tot de besluitvorming, is geen gezamenlijke besluitvorming.

[ISO Guide 73:2009, definitie 3.2.1]

1) Nederlandse voetnoot: de vertaling van deze opmerking wijkt enigszins af van de oorspronkelijke Engelse tekst, maar geeft wel de bedoelde strekking van de opmerking correct weer.

Bestelformulier

Stuur naar:

NEN Standards Products & Services
t.a.v. afdeling Klantenservice
Antwoordnummer 10214
2600 WB Delft

NEN Standards Products & Services

Postbus 5059
2600 GB Delft

Vlinderweg 6
2623 AX Delft

T (015) 2 690 390
F (015) 2 690 271

www.nen.nl/normshop

Ja, ik bestel

__ ex. NEN-ISO 31000:2009 nl Risicomanagement - Principes en richtlijnen € 144.38

Wilt u deze norm in PDF-formaat? Deze bestelt u eenvoudig via www.nen.nl/normshop

Gratis e-mailnieuwsbrieven

Wilt u op de hoogte blijven van de laatste ontwikkelingen op het gebied van normen, normalisatie en regelgeving? Neem dan een gratis abonnement op een van onze e-mailnieuwsbrieven. www.nen.nl/nieuwsbrieven

Gegevens

Bedrijf / Instelling

T.a.v. O M O V

E-mail

Klantnummer NEN

Uw ordernummer BTW nummer

Postbus / Adres

Postcode Plaats

Telefoon Fax

Factuuradres (indien dit afwijkt van bovenstaand adres)

Postbus / Adres

Postcode Plaats

Datum Handtekening

Retourneren

Fax: 015 2 690 271
E-mail: klantenservice@nen.nl
Post: NEN Standards Products & Services,
t.a.v. afdeling Klantenservice
Antwoordnummer 10214,
2600 WB Delft
(geen postzegel nodig).

Voorwaarden

- De prijzen zijn geldig tot 31 december 2018, tenzij anders aangegeven.
- Alle prijzen zijn excl. btw, verzend- en handelingskosten en onder voorbehoud bij o.m. ISO- en IEC-normen.
- Bestelt u via de normshop een pdf, dan betaalt u geen handeling en verzendkosten.
- Meer informatie: telefoon 015 2 690 391, dagelijks van 8.30 tot 17.00 uur.
- Wijzigingen en typefouten in teksten en prijsinformatie voorbehouden.
- U kunt onze algemene voorwaarden terugvinden op: www.nen.nl/leveringsvoorwaarden.