ISO 31000: nieuw referentiekader voor risicomanagement

Door ISO en IEC zijn eind 2009 twee nieuwe normen voor het onderwerp Risicomanagement gepubliceerd. Het gaat om twee generieke normen met termen en definities (ISO Guide 73) en richtlijnen voor de implementatie van risicomanagement (ISO 31000). In februari 2010 zijn de Nederlandse vertalingen verschenen: NEN-ISO 31000 *Risicomanagement – Principes en richtlijnen* en NPR-ISO Guide 73 *Risicomanagement – Verklarende woordenlijst*. De laatste is een tweetalige editie. Daarnaast is ook nog een richtlijn voor methoden voor risicobeoordeling uitgebracht, de ISO/IEC 31010 *Risk management – Risk assessment techniques*. Deze normenserie dient twee doelen. Ten eerste biedt het een algemeen kader voor organisaties die risicomanagement in de meeste brede zin in de praktijk willen brengen. Ten tweede dient het als paraplu voor allerlei sector- en onderwerpspecifieke ISO-normen op het gebied van risicomanagement.

Dick Hortensius, Senior-consultant NEN Managementsystemen en Ed Mallens, voorzitter normcommissie Risicomanagement en secretary-general PRIMO Europe

Door Nederland is een actieve bijdrage geleverd aan de totstandkoming van deze normen. Dit gebeurde door bespreking en becommentariëren van concepten in de normcommissie Risicomanagement. Daarnaast hebben de voorzitter en secretaris rechtstreeks geparticipeerd in de ISO werkgroep Risk Management.

Achtergrond

Het idee om een algemene ISO-norm voor risicomanagement te ontwikkelen bestond eigenlijk al geruime tijd. Ruim 10 jaar geleden stelde Japan voor om het onderwerp in het werkprogramma van ISO op te nemen. Aanleiding was de zware aardbeving in Kobe in 1995 die Japan confronteerde met het belang van het inschatten van risico's en het treffen van maatregelen om effecten van ongewenste gebeurtenissen te minimaliseren. De geesten binnen ISO waren toen echter nog niet rijp voor een norm of richtlijn voor risicomanagement in het algemeen. Die terughoudendheid was met name ingegeven door angst bij het bedrijfsleven dat zo'n norm tot nieuwe (ongewenste) certificatie-activiteiten zou gaan leiden. Daarom werd gekozen voor een 'veilige' oplossing, namelijk de ontwikkeling van een Guide met termen en definities op het gebied van risicomanagement. Dat werd uiteindelijk ISO/IEC Guide 73 *Risk management – Vocabulary – Guidelines for use in standards* die in 2002 werd gepubliceerd. De titel geeft al aan dat de Guide vooral bedoeld was om harmonisatie te bevorderen binnen het bouwwerk van ISO-normen. Er zijn namelijk tal van ISO-normen voor het managen en beoordelen van specifieke risico's in bepaalde sectoren. Enkele voorbeelden: ISO 14021 voor machineveiligheid, ISO 14971 voor medische hulpmiddelen, ISO 17776 voor offshore installaties en IEC 62198 voor risico's in projecten. Een uniform taalgebruik helpt dan al om vanuit die specifieke normen en richtlijnen een meer integrale kijk op risico's te ontwikkelen. Maar het gemis aan een algemene richtlijn voor risicomanagement werd door ISO/IEC Guide 73 niet weggenomen. Bij gebrek aan beter bleken veel organisaties hun toevlucht te nemen tot de Australisch-Nieuwzeelandse norm AZ/NZS 4360 *Risk management*. Daarnaast sprong bijvoorbeeld de Europese organisatie Ferma in het door ISO opengelaten gat met de

publicatie van haar eigen Risk Management Standard. Het was dus eigenlijk onontkoombaar dat het onderwerp terug zou komen op de agenda van ISO.

Nieuw voorstel

In 2005 werd door Japan en Australië gezamenlijk het voorstel gedaan om een algemene ISO-richtlijn voor de principes en implementatie van risicomanagement te ontwikkelen. Van meet af aan werd duidelijk gemaakt dat de beoogde richtlijn niet bedoeld was als basis voor certificatie. Daarnaast werd aangegeven dat het proces van risicomanagement centraal zou moeten staan in de richtlijn en niet een risicomanagementsysteem. Nederland heeft toen positief gereageerd op dat voorstel met de kanttekening dat de richtlijn een paraplufunctie zou moeten hebben voor bestaande en toekomstige ISO-normen en consistent zou moeten zijn met door en voor andere sectoren ontwikkelde normen, zoals die in de financiële sector. Het voorstel werd door de vereiste meerderheid van ISO-leden gesteund en medio 2005 werd de ISO-werkgroep *Risk management* opgezet. Voorzitter van die werkgroep was Kevin Knight uit Australië en het secretariaat wordt verzorgd door het Japanse normalisatie-instituut. In de werkgroep namen enkele tientallen experts deel uit ca. 25 verschillende landen en vanuit een aantal technische commissies van ISO en IEC. Nederland werd in de werkgroep vertegenwoordigd door Dick Hortensius (NEN) en Ed Mallens. Na 6 vergaderingen en een aantal stem – en commentaarrondes zijn in november 2009, ISO 31000 *Risk management – Principles and guidelines* en de herziene editie van ISO Guide 73 *Risk management – Vocabulary* gepubliceerd. Parallel is door ISO en IEC ook de gezamenlijke publicatie ISO/IEC 31010 *Risk management – Risk assessment techniques* uitgebracht. In de volgende paragrafen worden de inhoud en betekenis van deze normen toegelicht.

Wat is een risico?

De ISO-werkgroep ging in eerste instantie aan de slag met de principes en richtlijnen voor risicomanagement. Daarbij werd al snel duidelijk dat de terminologie in ISO/IEC Guide 73 uit 2002 niet goed aansloot bij de nieuwste inzichten in risicomanagement en het beoogde brede toepassingsgebied van ISO 31000. Daarom werd ook een herziening van Guide 73 ter hand genomen. De uiteindelijke Guide bevat 50 termen en definities, waarvan de belangrijkste hier kort worden toegelicht.

In het kader is de definitie van de term risico opgenomen met de daarbij behorende opmerkingen. Over die definitie is gedurende een paar vergaderingen langdurig van gedachten gewisseld. Belangrijk uitgangspunt was dat de definitie niet (alleen) het negatieve karakter van risico's (kans op schadelijke effecten) zou moeten weergeven, maar risico als neutraal begrip neerzetten (kansen en bedreigingen). Dit sluit aan bij risicomanagement als basis van ondernemen, want 'ondernemen is risico nemen'. Dat is het omgaan met onzekerheden die positieve en negatieve effecten op de bedrijfsresultaten en daarmee het succes van de organisatie kunnen hebben. De eerste

Definitie van risico

Risico is het effect van onzekerheid op het behalen van doelstellingen.

Opmerking 1 Een effect is een afwijking van de verwachting - positief en/of negatief;

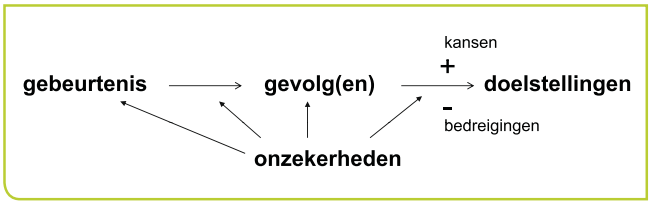
Opmerking 2 Doelstellingen kunnen worden gekenmerkt door verschillende aspecten (bijvoorbeeld financiële, arbo- of milieudoelen) en kunnen betrekking hebben op verschillende niveaus (zoals strategisch, organisatiebreed, een project, product of proces);

Opmerking 3 Een risico wordt vaak gekarakteriseerd door verwijzing naar mogelijke gebeurtenissen en gevolgen of een combinatie daarvan;

Opmerking 4 Risico wordt vaak uitgedrukt als een combinatie van de gevolgen van een gebeurtenis (met inbegrip van wijzigingen in omstandigheden) en de bijbehorende waarschijnlijkheid 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.

opmerking bij de definitie benadrukt dat nog eens. Het begrip 'risico' moet breder worden gezien dan oorzaak en effect en kans x gevolg. De opmerkingen 3 en 4 bij de definitie zijn bedoeld om de relatie te leggen met die meer 'klassieke' omschrijvingen van het begrip risico, die natuurlijk nog steeds kunnen worden gebruikt om in specifieke situaties een risico kwalitatief of kwantitatief uit drukken. De tweede opmerking geeft de beoogde reikwijdte van risicomanagement volgens ISO 31000 weer: alle typen risico's op alle denkbare niveaus van een organisatie. Van de arborisico's verbonden aan een bepaalde machine tot de strategische risico's op concernniveau. Figuur 1 laat risico's zien die te maken hebben met de onzekerheden van het optreden van bepaalde gebeurtenissen (of optredende veranderingen in omstandigheden), de mogelijke consequenties daarvan en het mogelijk effect op de doelstellingen van een organisatie (of project, proces, product etcetera). Risicomanagement is erop gericht goed inzicht te krijgen in die componenten van risico's en maatregelen te treffen om de negatieve gevolgen tegen te gaan en de kansen optimaal te benutten.



Figuur 1 – Het risicoconcept volgens ISO Guide 73 en ISO 31000

Eenduidig begrippenkader

Risicomanagement omvat de gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot risico's. Deze definitie is rechtstreeks ontleend aan de definitie voor kwaliteitsmanagement uit ISO 9000. Belangrijk is vervolgens hoe risicomanagement wordt ingebed in een organisatie. Daarbij is er bewust voor gekozen om het begrip risicomanagementsysteem te vermijden. De ervaring leert dat kwaliteits- en milieumanagementsystemen te vaak als aparte systemen in een organisatie worden geïmplementeerd los van het 'echte' managementsysteem. Volgens één van de principes in ISO 31000 is risicomanagement echter pas effectief als het een integraal onderdeel is van de processen in de organisatie. Daarom wordt het begrip Risk **management framework** (raamwerk voor risicomanagement) gehanteerd. Het gaat daarbij om de grondbeginselen en organisatorische maatregelen die ervoor zorgdragen dat risicomanagementprocessen door de gehele organisatie worden toegepast. Met behulp van dit raamwerk moet risicomanagement worden ingebed in de algehele strategische en operationele activiteiten van een organisatie.

Het **risicomanagementproces** omvat de systematische aanpak om risico's te identificeren, analyseren, evalueren, behandelen en monitoren, maar ook de consultatie en communicatie gedurende dat proces. Het raamwerk moet ervoor zorgen dat de resultaten van afzonderlijke risicom anagementprocessen zo nodig worden geconsolideerd op het juiste organisatieniveau als basis voor operationele of strategische besluitvorming.

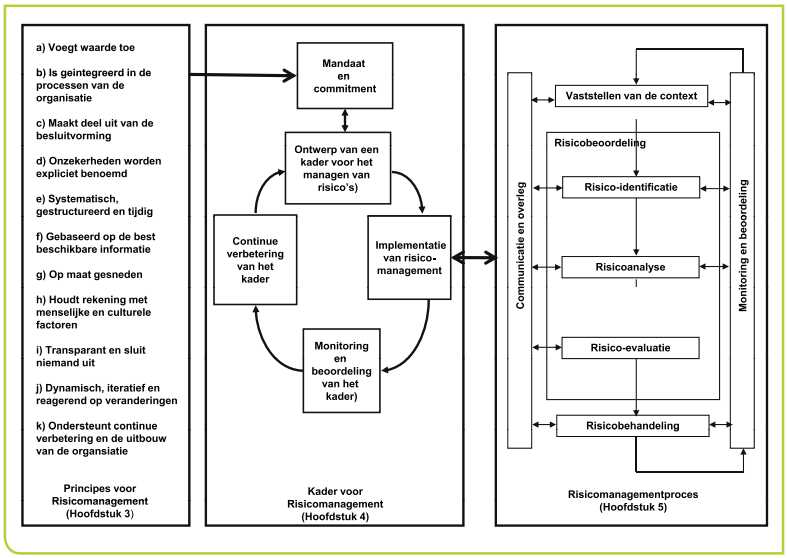
Door het definiëren van begrippen als **externe en interne context, communicatie en consultatie** en **stakeholder** wordt duidelijk dat risicomanagement veel zo niet alles te maken heeft met een goed (in)zicht op wat er speelt in de omgeving van een organisatie en met interactie met belanghebbende partijen. Uiteraard besteedt ISO Guide 73 ook aandacht aan de 'klassieke' begrippen op het gebied van risicobeheersing, zoals gebeurtenis en consequentie, waarschijnlijkheid, risico-identificatie, risicoanalyse, risico-evaluatie and risicobeoordeling. Daarmee biedt ISO Guide 73 een goede basis voor eenduidige communicatie over risico's en risicomanagement tussen organisaties, over landsgrenzen en door alle verschillende betrokken vakdisciplines heen.

Scope, doelgroep en voordelen

ISO 31000 beschrijft principes en generieke richtlijnen voor de implementatie van risicomanagement. De richtlijn is bedoeld voor alle typen organisaties, ongeacht grootte en aard van activiteiten, en kan worden toegepast op een breed scala van activiteiten, projecten, producten, assets, maar is vooral gericht op organisatie-breed risicomanage-ment. De richtlijn laat nadrukkelijk ruimte voor maatwerk omdat wordt onderkend dat risicomanagement 'tailor-made' moet zijn. De doelgroep van de richtlijn is logischerwijs ook heel divers: verantwoordelijken voor risicomanagement binnen organisaties als geheel of voor specifieke onderdelen of activiteiten, maar ook personen/organisaties

die er op toe moeten zien dat een organisatie haar risico's goed managed of de aanpak daarvan moet beoordelen.

Daarnaast is ISO 31000 bedoeld voor degenen die binnen of buiten ISO normen en richtlijnen op het gebied van risicomanagement ontwikkelen. De voordelen van toepassing van risicomanagement zijn velerlei, bijvoorbeeld het verbeteren van de 'corporate governance' en daarmee van vertrouwen dat stakeholders in de organisatie hebben. De grotere weerstand tegen bedreigingen ('resilience'). Beter inzicht in de kansen voor ontwikkeling en groei. Maar ook goede besluitvorming, naleving van wet- en regelgeving, verbeterde arbo- en milieuveiligheid, het voorkomen van calamiteiten en 'business continuity'.
ISO 31000 bestaat uit drie hoofdonderdelen: de principes voor risicomanagement, het risk management framework en het risicomanagementproces. De onderlinge relatie wordt aangegeven in figuur 2.



Figuur 2 – Onderlinge samenhang onderdelen van ISO 31000

Principes van risicomanagement

In het eerste 'inhoudelijke' hoofdstuk van ISO 31000 worden 11 principes genoemd waaraan risicomanagement zou moeten voldoen, wil het een effectief instrument worden voor een organisatie. In het kader staan de principes op een rijtje; in ISO 31000 wordt elk principe kort toegelicht. Gezamenlijk bestrijken deze principes een paar belangrijke kenmerken van risicomanagement:

- het voegt waarde toe en draagt bij aan verbetering van de organisatie;
- het is een integraal onderdeel van de (besluitvormings)-processen;
- het is maatwerk, past bij de context van de organisatie en volgt de veranderingen;
- het is een systematisch en op feiten gebaseerd proces;
- het is open en transparant en houdt rekening met menselijke en culturele factoren.

De eerste drie kenmerken vormen de basis voor het kader voor risicomanagement en de laatste twee zijn vooral terug te vinden in het risicomanagementproces.

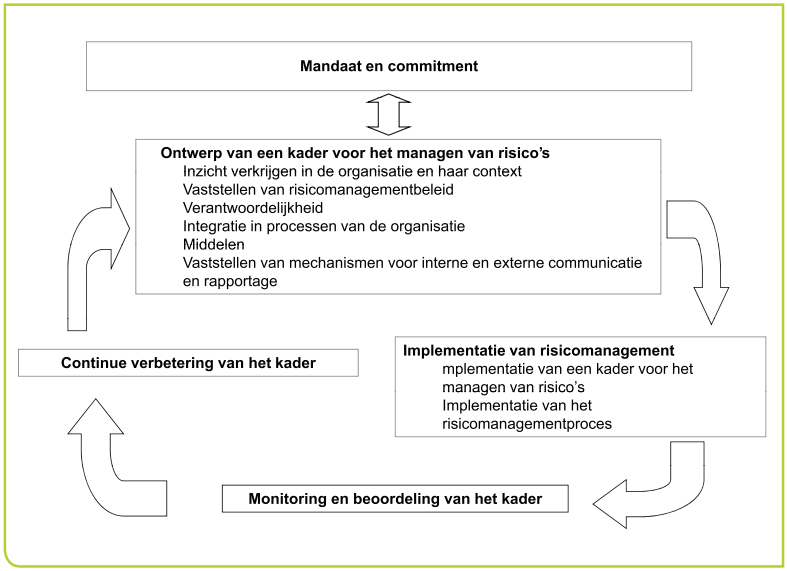
Risicomanagement

a) voegt waarde toe en zorgt voor behoud van waarde;
b) maakt integraal deel uit van alle processen in de organisatie;
c) maakt deel uit van de besluitvorming;
d) benoemd expliciet onzekerheid;
e) is systematisch, gestructureerd en tijdig;
f) is gebaseerd op de beste beschikbare informatie;
g) is op maat toegesneden;
h) houdt rekening met menselijke en culturele factoren;
i) is dynamisch, iteratief en reageert op verandering;
j) ondersteunt continue verbetering in de organisatie.

Raamwerk voor risicomanagement

In vroege concepten van ISO 31000 stond vooral het risicomanagementproces centraal en werd nauwelijks aandacht besteed aan de inbedding van (de resultaten van) dat proces in het bredere organisatorische kader. Dat had te maken met het feit dat de Australisch-Nieuwzeelandse norm AZ/NZS 4360 een belangrijk uitgangspunt in de discussies was en die norm beschrijft eigenlijk alleen het risicomanagementproces. De tweede reden was het uitgangspunt dat ISO 31000 geen 'managementsysteemnorm' zou moeten worden.

Onder andere door inbreng van de Nederlandse vertegenwoordigers in de ISO-werkgroep is het Risk management framework geïntroduceerd. Dit is het kader dat ervoor moet zorgen dat risicomanagementprocessen zijn ingebed in het algehele management(structuur) en de besluitvormingsprocessen van een organisatie en dat ze worden aangestuurd vanuit een duidelijke visie en beleid op de functie van risicomanagement voor de organisatie. Daartoe bevat het raamwerk de elementen zoals weergegeven in figuur 3.



Figuur 3 – Het raamwerk voor risicomanagement uit ISO 31000

Het zal duidelijk zijn dat het cyclische proces en de verschillende componenten veel overeenstemming vertonen met de structuur en onderdelen van een 'ISO-managementsysteem'. Daaruit blijkt dat bij het formuleren van de randvoorwaarden om iets goed en blijvend goed te regelen in een organisatie, steeds dezelfde en zichzelf bewezen aanpak terugkomt. In lijn met de principes voor risicomanagement wordt in de tekst benadrukt dat het framework behulpzaam moet zijn om risicomanagement te integreren in de algehele managementstructuur van de organisatie en dat een organisatie daartoe de elementen moet aanpassen aan de eigen specifieke situatie.

Kortom, het is geen blauwdruk voor 'risicomanagement-systeem', maar een handvat voor integratie. Als het framework wordt vergeleken met bijvoorbeeld de eisen aan een kwaliteitsmanagementsysteem in ISO 9001 of het milieumanagementsysteem in ISO 14001, vallen een paar zaken op. Het expliciete mandaat en commitment van het (top)management, de oriëntatie op de interne en externe context van de organisatie, de integratie in de bedrijfsprocessen en de interne en externe communicatie- en rapportagemechanismen. Dit sluit aan bij eerder genoemde principes van risicomanagement.

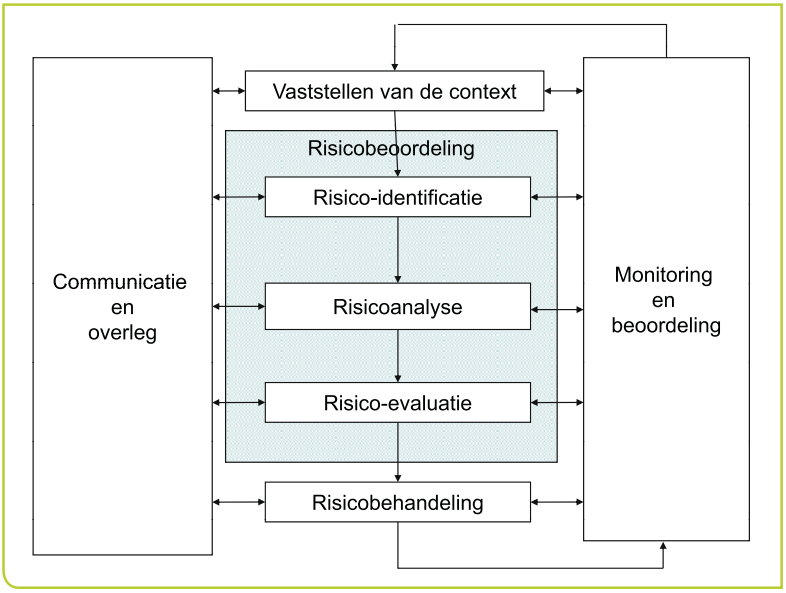
Risicomanagementproces(sen)

Risicomanagement krijgt concreet gestalte door uitvoering van het zogenoemde risicomanagementproces. Dit is breder dan een risico-analyse of -beoordeling, zoals blijkt uit de in figuur 4 weergegeven stappen en onderdelen van dat proces.

n het hart van het proces zitten de bekende stappen van het identificeren, analyseren en evalueren van risico's verbonden aan proces, product, project of organisatie als geheel. Die stappen vormen tezamen de risicobeoordeling. Die beoordeling kan alleen goed worden uitgevoerd als de context en scope zijn bepaald. Die context wordt ten dele ontleend aan het Risk management framework, maar voor de risicobeoordeling van een specifieke situatie kan en moet die context gedetailleerder worden bekeken.

Bijvoorbeeld de specifieke doelstellingen van een project, de daarbij betrokken interne en externe partijen, de technologische en juridische context waarin het project wordt uitgevoerd etc. Aan zo'n contextbepaling worden bijvoorbeeld specifieke criteria ontleend om de risico's te beoordelen, uiteraard binnen de algemene 'risk appetite' van de organisatie. Vanuit die contextbepaling wordt ook duidelijk welke personen en organisaties moeten worden geconsulteerd of betrokken bij de risicobeoordeling en met wie op welke wijze moet worden gecommuniceerd over de aanpak en resultaten.

Op basis van de beoordeling wordt besloten of en zo ja hoe het risico wordt 'behandeld' (engels: treated). Dat kan variëren van het volledig vermijden van het risico door de activiteit waarmee het risico verbonden is te beëindigen, via het beïnvloeden van kans op optreden of effect ervan tot en met het accepteren van het risico zonder verdere aanpassingen. Vervolgens is monitoring en herbeoordeling



Figuur 4 – Het risicomanagementproces volgens ISO 31000

van de ontstane situatie belangrijk om na te gaan of toegepaste beheersmaatregelen effectief zijn of dat de context verandert waardoor de bepaalde risico's anders moeten worden gewaardeerd en aangebrachte controls moeten worden aangepast. De activiteiten 'consultatie en communicatie' en 'monitoring en review' zijn ook belangrijke schakels naar het raamwerk voor risicomanagement die ervoor zorgen dat de resultaten van specifieke risicomanagementprocessen worden gerapporteerd en geconsolideerd naar het gewenste niveau van de organisatie.

Methoden voor risicobeoordeling

Zoals eerder aangegeven is parallel aan ISO 31000 en de ISO Guide 73 door IEC en ISO de ISO/IEC 31010 gepubliceerd met een overzicht van technieken voor risicobeoordeling. Deze norm beschrijft de basiskenmerken van 28 verschillende technieken voor risicobeoordeling, variërend van FMEA en HAZOP tot scenario-analyses en Delphi-technieken. De methoden worden op twee manieren geclassificeerd. Ten eerste op welke stappen van het risicobeoordelingsproces ze betrekking hebben: risico-identificatie, effectanalyse, kansanalyse, risicoschatting en risico-evaluatie. Ten tweede op de volgende parameters: benodigde middelen en expertise, de mate van zekerheid en exactheid van de uitkomsten en de geschiktheid voor complexe risicosituaties. Op die manier ontstaat een handig spoorboekje om een weg te vinden in de vele methoden en technieken van risicobeoordeling en is het een praktische aanvulling op ISO 31000.

Betekenis van de ISO 31000 en de vernieuwde Guide 73 voor het vak risicomanagement

Door de vaststelling van beide documenten ontstaat een consistent denkraam met duidelijk verklaarde begrippen die laat zien wat risicomanagement is. Hoe daar invulling aan te geven is aan de verantwoordelijken, gebruikers, toepassers en opleiders van risicomanagement.

Vier belangrijkste functies van ISO 31000

ISO 31000 kan naar ons idee ten minste vier functies hebben voor een organisatie:

1. Als paraplu en integratiekader voor afzonderlijke managementsystemen voor specifieke risico's, zoals kwaliteits-, milieu- en arbomanagement;
2. Als brug tussen het management van financiële en fysieke risico's; de eerste categorie is vaak het domein van controllers en internal audit en de tweede categorie dat van de KAM-manager;
3. Als handvat voor organisaties die aan het begin staan van het invoeren van organisatiebreed risicomanagement; en
4. Tenslotte als spiegel voor organisaties die al een eind op weg zijn met risicomanagement en eventueel een ander model (Coso, M_o_R) gebruiken: wat kunnen zij nog leren en verbeteren op basis van ISO 31000?

In internationaal verband is er nu voor het eerst een actueel eenduidig referentie- en begrippenkader beschikbaar voor iedereen die werkzaam is in het vakgebied van risicomanagement en voor al degenen die kansen en bedreigingen serieus neemt in zijn dagelijkse praktijk!

Meer informatie

Voor meer informatie kunt u contact opnemen met Dick Hortensius, telefoon (015) 2 690 115 of e-mail dick.hortensius@nen.nl.