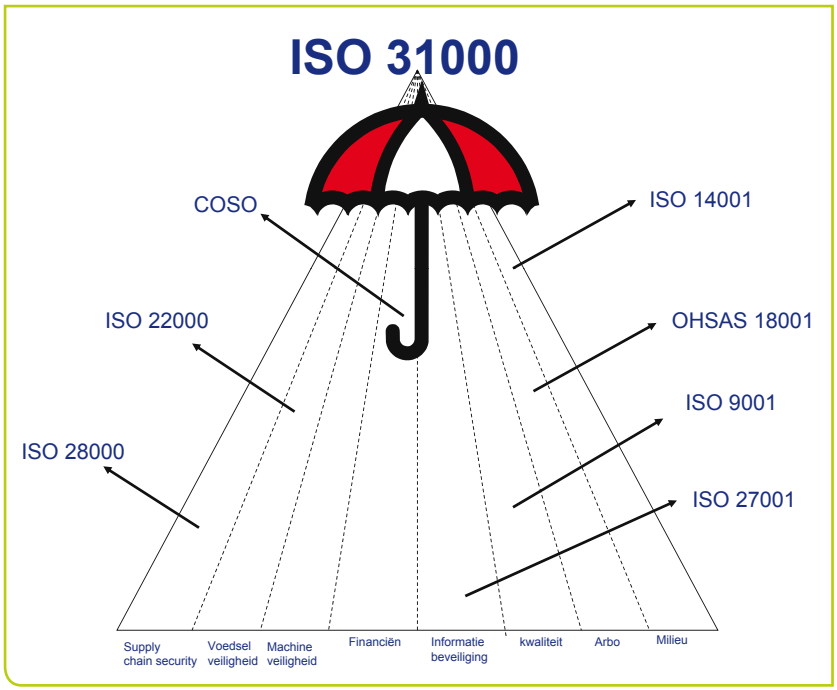
# ISO 31000 als kader voor integratie

Eind vorig jaar is ISO 31000 *Risicomanagement – Principes en richtlijnen* gepubliceerd. Het is de eerste ISO-norm voor organisatiebreed risicomanagement. Elders in deze KAMNieuwsbrief wordt uitgebreid ingegaan op de inhoud en betekenis van deze norm. Een van de functies van ISO 31000 die daarin wordt genoemd is die van paraplu en integratiekader voor afzonderlijke managementsystemen voor specifieke risico's, zoals kwaliteits-, milieu- en arbomanagement. In dit artikel wordt nagegaan welke aanknopingspunten ISO 31000 daarvoor biedt.

*Dick Hortensius, Senior-consultant NEN Managementsystemen*

## Managementsystemen voor specifieke risico's

ISO 9001 voor kwaliteitsmanagement, ISO 14001 voor milieumanagement, ISO 22000 voor voedselveiligheids-management en OHSAS 18001 voor arbomanagement, het zijn eigenlijk allemaal normen die beschrijven hoe een organisatie een specifiek risico moet managen.
Bij kwaliteitsmanagement gaat het om de risico's dat producten en diensten niet aan de eisen van de klant en van toepassing zijnde wettelijke eisen voldoen. Bij milieumanagement om risico's dat schade aan het milieu wordt toegebracht met als mogelijk gevolg aansprakelijk-heidsclaims, imagoschade, strafrechtelijke vervolging, etcetera. Bij voedselveiligheidsmanagement om risico's dat producten schadelijk zijn voor de gezondheid van de consument. Zo is elke managementsysteemnorm te koppelen aan een specifiek risico waar de organisatie rekening mee moet houden.




*Figuur 1 – ISO 31000 als koepel*

Die normen bevatten op hoofdlijnen allemaal dezelfde componenten:

- Beleid en doelstellingen;
- Vaststellen van eisen waaraan moet worden voldaan;
- Risicoanalyse en vaststelling beheersmaatregelen;
- Organisatie, middelen, competenties;
- Procesbeheersing;
- Monitoring, analyse en verbetering.

## Van verzuiling naar integratie

In het verleden zijn binnen veel organisaties allerlei verzuilde managementsystemen ontstaan, gekoppeld aan de verschillende normen met eigen coördinatoren, vaak vakspecialisten. Die systemen stonden vaak los van elkaar en ook nog eens los van het 'echte managementsysteem' van de organisatie. Dat 'echte' systeem is gekoppeld aan het strategisch en financieel management, het domein van de directie en de controller van de organisatie.

Inmiddels is het besef gegroeid dat een organisatie bij het implementeren van een managementsysteemnorm die norm niet als een recept moet gebruiken om een nieuw managementsysteem in de organisatie neer te zetten. Het gaat erom dat wordt nagegaan waar het al bestaande 'echte' managementsysteem (formeel of informeel) moet worden aangepast of aangevuld om te kunnen claimen dat aan bijvoorbeeld ISO 14001 wordt voldaan. Als dat

goed gebeurt, worden twee vliegen in een klap geslagen: verzuiling (en daarmee versnippering en inefficiënties) wordt tegengegaan en het betreffende risico/aspect wordt meegenomen in het algehele management van de organisatie (op strategisch, tactisch en operationeel niveau).

## Handvatten in ISO 31000

De praktijk is echter weerbarstig en er zijn nog veel organisaties met niet of slechts gedeeltelijk geïntegreerde KAM-systemen die vaak ook nog aan de zijlijn opereren. ISO 31000 biedt een aantal aanknopingspunten voor een KAM-manager om dit probleem bij de kop te pakken:

1. ISO 31000 biedt een algemene 'taal' voor het (risico)management van een organisatie. Het kan daarmee helpen om de aandachtspunten en activiteiten in de afzonderlijke managementsystemen onder één noemer te brengen;
2. ISO 31000 steekt in op een strategisch niveau en benadrukt het belang van een externe en interne oriëntatie ('bepaling van de context') om na te gaan in wat voor 'business environment' wordt geopereerd, welke belangrijke ontwikkelingen zich voordoen, met welke stakeholders rekening moet worden gehouden en wat de cultuur van de organisatie is. Allemaal zaken die bepalen met wat voor risico's de organisatie rekening moet houden, ofwel met welke onzekere factoren die het behalen van de doelstellingen van de organisatie kunnen beïnvloeden.
3. ISO 31000 benadrukt het belang van integratie van risicomanagement in de 'governance' van een organisatie: het moet onderdeel worden van alle besluitvormings- en besturingsprocessen, onderdeel van de cultuur en houding van een organisatie. De richtlijn beschrijft dan ook niet een apart risicomanagementsysteem, maar benoemt de elementen van een 'raamwerk voor risicomanagement' wat moet helpen deze integratie in het algemene managementsysteem vorm te geven.
4. ISO 31000 geeft het belang aan van commitment en actieve betrokkenheid van het topmanagement als randvoorwaarde voor effectief risicomanagement. Het gaat niet alleen om toedeling van 'responsibilities' (verantwoordelijkheden) in de organisatie, maar ook om het vastleggen van 'accountabilities' (het afleggen van rekenschap): risicomanagement is geen vrijblijvende zaak.
5. ISO 31000 beschrijft een generiek risicomanagement-proces, bestaande uit een risicobeoordeling, treffen van beheersmaatregelen (risk controls) en monitoring van de effectiviteit daarvan. Daarbjj is de context weer van belang: specifieke stakeholders en van toepassing zijnde (wettelijke) eisen en interne en externe communicatie en rapportage. De risicomanagementprocessen worden aangestuurd vanuit het raamwerk, ofwel vanuit het algemene managementsysteem van de organisatie en de resultaten teruggesluisd naar de relevante besluitvormingsprocessen op alle niveaus.

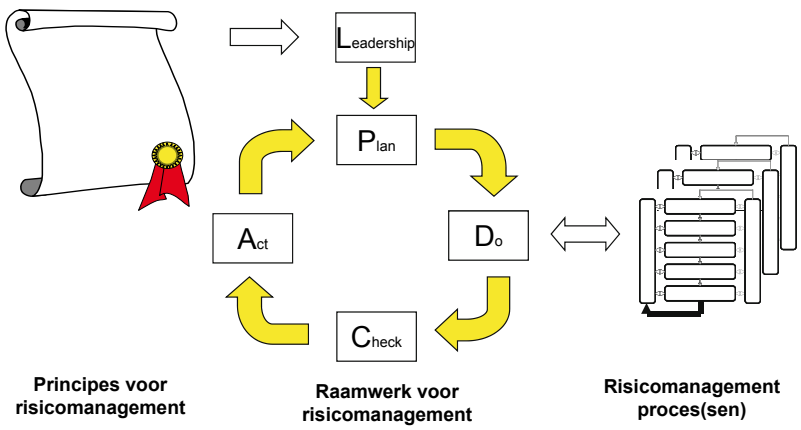
Deze vijf handvatten in ISO 31000 kan de KAM-manager gebruiken om bestaande aparte systemen of aanpakken te integreren en onderdeel te laten worden van de algehele besturing van de organisatie.

## ISO 31000 als kader

In figuur 2 op de volgende pagina zijn de hoofdonderdelen van ISO 31000 weergegeven. Alle drie kunnen ze gebruikt worden voor integratie van afzonderlijke management-systemen in het algemene managementsysteem van een organisatie.

De **principes voor risicomanagement** zijn te veralgemeniseren naar de principes van goed management en kunnen worden gebruikt als toetssteen voor de opzet en effectiviteit van het geïntegreerde systeem. Het **kader voor risicomanagement** geeft de aanknopingspunten om afzonderlijke managementsysteemelementen te integreren in het besturingssysteem van de organisatie.

De **risicomanagementprocessen** geven de mogelijkheid om op elk gewenst niveau (proces, product, project, afdeling), (specifieke) risico's te beoordelen en beheersmechanismen vast te stellen, te monitoren en te onderhouden. Het kader voor risicomanagement zorgt ervoor dat beoordeling van risico's plaatsvindt vanuit het algemene risicobeleid en de 'risk appetite' van de organisatie (de mate waarin een organisatie risico's wil nemen). Het kader zorgt er ook voor dat integrale afweging van verschillende types risico's op verschillende niveaus kan plaatsvinden en dat de uitkomsten daarvan worden meegenomen bij besluitvorming en strategiebepaling van de organisatie.




*Figuur 2 – Hoofdonderdelen van ISO 31000*

Een groot deel van de eisen van de huidige normen voor managementsystemen zit op het niveau van het risicomanagementproces. Dit is voor ISO 9001 en ISO 14001 globaal aangegeven in onderstaande tabel. Het risicomanagementproces is het niveau waarop meer uniformiteit tussen de verschillende deelsystemen kan worden bereikt en een geïntegreerde benadering kan worden toegepast. De risico-optiek zorgt er ook voor dat kwaliteits-, milieu, arbo- en andere aspecten worden beoordeeld in het licht van de doelstellingen van de organisatie en de wensen en eisen van haar stakeholders. Het risicomanagementkader zorgt voor uniformiteit in de aansturing van die processen en is de basis voor een uniform beoordelingskader voor de verschillende typen risico's. En niet in de laatste plaats zorgt dit kader voor integratie met de 'governance' van de organisatie en de koppeling met beleid en doelstellingen op het hoogste niveau.

## Afsluiting

In dit artikel zijn enkele aanknopingspunten gegeven voor geïntegreerde toepassing van normen voor management-systemen met ISO 31000 als integratiekader. Het voordeel hiervan is dat het de risicogerichtheid van de afzonderlijke systemen expliciet maakt, koppelt aan het beleid en de doelstellingen van de organisatie en integreert met het algehele managementsysteem van de organisatie.

## Meer informatie

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

### Risicomanagementproces

| ISO 31000 | ISO 9001 | ISO 14001 |
|---|---|---|
| 5.2 Communicatie en overleg | 5.5.3 Interne communicatie<br>7.2.3 Communicatie met de klant | 4.4.3 Communicatie |
| 5.3 Vaststellen van de context | 7.2.1 Bepaling van producteisen | 4.3.2 Wettelijke en andere eisen |
| 5.4 Risicobeoordeling | 7.2.2 Beoordeling van producteisen | 4.3.1 Milieuaspecten |
| 5.5 Risicobehandeling | 7.3 Ontwerp en ontwikkeling<br>7.4 Inkoop<br>7.5 Productie en leveren van diensten | 4.4.6 Beheersing van werkzaamheden<br>4.4.7 Noodsituaties |
| 5.6 Monitoring en beoordeling | 8 Meting, analyse en verbetering | 4.5.1 Monitoring en meting<br>4.5.4 Afwijkingen, corrigerende en preventieve maatregelen |
| 5.7 Registratie van het proces | 4.2.4 Beheersing van registraties | 4.5.4 Beheersing van registraties |

*Tabel – Correspondentie tussen het generieke risicomanagementproces uit ISO 31000 en ISO 9001 en ISO 14001*