Belgische norm

ISO 31000:2018

NBN ISO 31000:2018

Risicomanagement - Richtlijnen (ISO 31000:2018)

Geldig vanaf 28-02-2018

Vervangt NBN ISO/DIS 31000:2017, NBN ISO 31000:2014 en NBN ISO 31000 NL:2014

ICS: 03.100.01

Bureau voor Normalisatie
Jozef II-straat 40 bus 6
1000 Brussel

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

Nationaal voorwoord

Deze norm is opgesteld door de internationale Technische Commissie ISO/TC 262 “Risk management”. Verdere details wat dat betreft worden verstrekt in het Voorwoord bij deze norm.

De internationale norm werd door het Bureau voor Normalisatie (NBN) ongewijzigd geregistreerd en gepubliceerd als Belgische norm.

De Nederlandstalige versie van deze norm is opgesteld door het NEN.

Nederlands voorwoord (NEN)

Dit document bevat de vertaling in het Nederlands van de internationale norm ISO 31000:2018. De internationale norm heeft de status van Nederlandse norm.

Deze NBN-versie is grotendeels gebaseerd op de NEN-versie, maar houdt tegelijk rekening met een aantal verschillen op het vlak van terminologie tussen Nederland en Vlaanderen. De onderstaande synoniemenlijst vermeldt de termen waarvoor het NBN een afwijkende keuze heeft gemaakt.

Synoniemenlijst

Engelse term	*Nederlandse term in de NEN-versie*	*Nederlandse term in de NBN-versie*
commitment	commitment	betrokkenheid

Inhoud

Voorwoord

ISO (International Organization for Standardization) is een wereldwijde federatie van nationale normalisatie-instituten (de ISO-leden). Het opstellen van 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. Ook internationale organisaties, zowel overheidsinstanties als ngo's, nemen in samenwerking met ISO deel aan deze werkzaamheden. ISO werkt nauw samen met de International Electrotechnical Commission (IEC) inzake alle elektrotechnische normalisatie.

De procedures die zijn gebruikt voor het ontwikkelen van dit document en de procedures die zijn bedoeld voor het verdere onderhoud ervan, worden beschreven in deel 1 van de ISO/IEC-richtlijnen. Hierbij wordt met name gewezen op de verschillende goedkeuringscriteria die nodig zijn voor de verschillende soorten ISO-documenten. Dit document is opgesteld volgens de redactionele regels die in deel 2 van de ISO/IEC-richtlijnen zijn opgenomen (zie www.iso.org/directives).

Er wordt gewezen op de mogelijkheid dat sommige elementen van dit document onderwerp zijn van patentrechten. ISO is niet verantwoordelijk voor identificatie van dergelijke patentrechten. Nadere informatie over eventuele patentrechten die zijn geïdentificeerd tijdens het ontwikkelen van het document, is te vinden in de inleiding en/of de ISO-lijst met ontvangen patentverklaringen (zie www.iso.org/patents).

Eventuele handelsnamen die in dit document worden gebruikt, zijn verstrekt ter informatie voor het gemak van de gebruiker en houden geen aanbeveling in.

Uitleg over de vrijwillige aard van normen, de betekenis van ISO-specifieke termen en uitdrukkingen met betrekking tot conformiteitsbeoordeling, evenals informatie over hoe ISO voldoet aan de in de Technical Barriers to Trade (TBT) vervatte beginselen van de Wereldhandelsorganisatie (WTO), wordt gegeven op de volgende URL: www.iso.org/iso/foreword.html.

Dit document is opgesteld door Technische Commissie ISO/TC 262, *Risk management*.

Deze tweede editie herroept en vervangt de eerste editie (ISO 31000:2009), die technisch is herzien.

De belangrijkste wijzigingen ten opzichte van de vorige editie zijn:

— herijking van de principes van risicomanagement, die de belangrijkste criteria zijn voor het succes ervan;

— benadrukken van het leiderschap door de directie en de integratie van risicomanagement, te beginnen bij de governance van de organisatie;

— meer nadruk op de iteratieve aard van risicomanagement, waarbij wordt opgemerkt dat nieuwe ervaringen, kennis en analyse tijdens elke fase van het proces tot een herziening van proceselementen, maatregelen en beheersmaatregelen kunnen leiden;

— het stroomlijnen van de inhoud met meer aandacht voor het behouden van een open systeemmodel dat past bij een veelheid aan behoeften en contexten.

Inleiding

Dit document is bedoeld voor gebruik door personen die waarde creëren en voor behoud van waarde in organisaties zorgen door risico's te managen, besluiten te nemen, doelstellingen vast te stellen en te bereiken en prestaties te verbeteren.

Ongeacht type en omvang van de organisatie, wordt elke organisatie geconfronteerd met externe en interne factoren en invloeden die ertoe leiden dat het onzeker is of zij haar doelstellingen zal behalen.

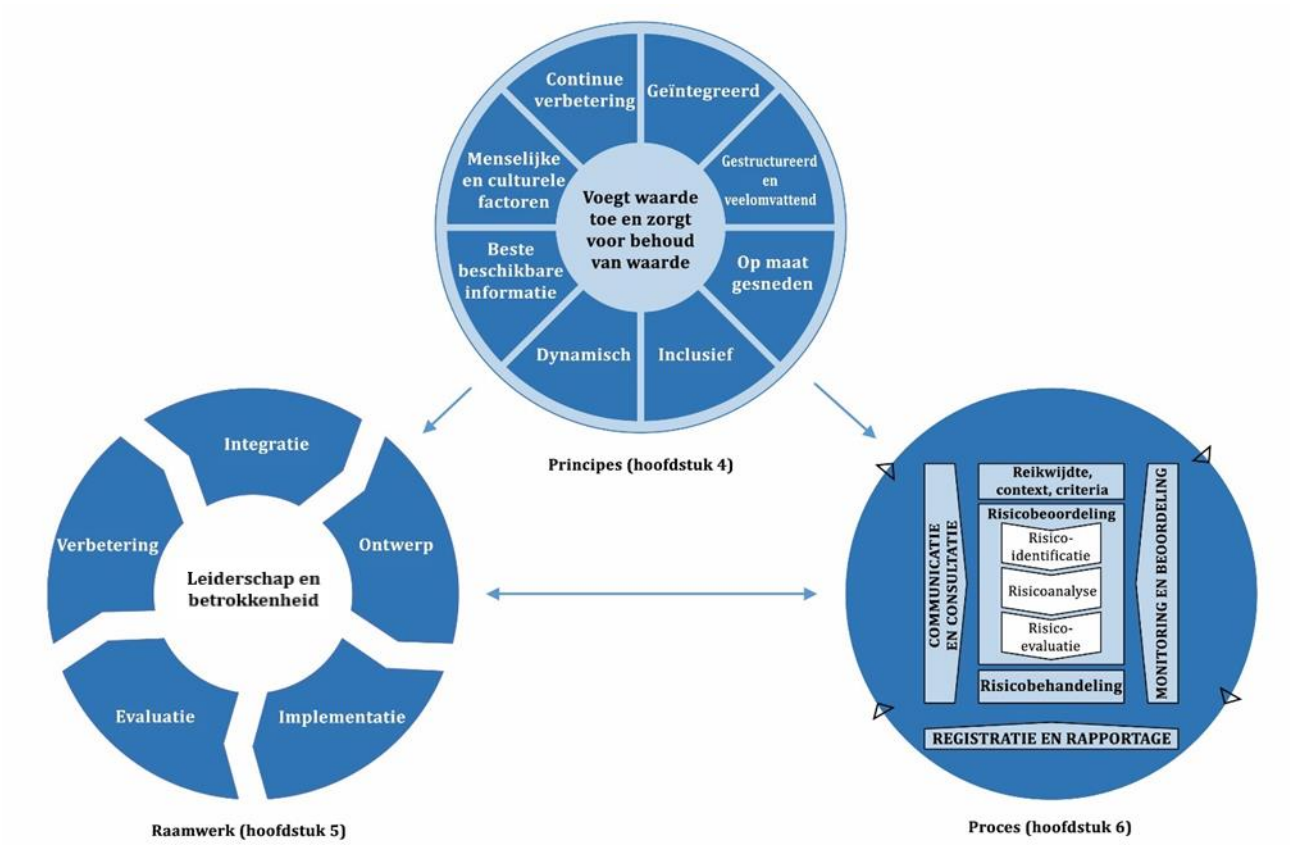
Het managen van risico's is iteratief en helpt organisaties bij het vaststellen van strategie, het bereiken van doelstellingen en het nemen van onderbouwde besluiten.

Het managen van risico's maakt deel uit van governance en leiderschap en is essentieel voor hoe de organisatie op alle niveaus bestuurd wordt. Het draagt bij aan de verbetering van managementsystemen.

Het managen van risico's maakt deel uit van alle activiteiten die verband houden met een organisatie, en omvat interactie met belanghebbenden.

Bij het managen van risico's wordt rekening gehouden met de externe en interne context van de organisatie, met inbegrip van menselijk gedrag en culturele factoren.

Het managen van risico's is gebaseerd op de principes, het raamwerk en het proces zoals beschreven in dit document en geïllustreerd in figuur 1. Deze componenten kunnen al geheel of gedeeltelijk binnen de organisatie aanwezig zijn, maar toch kan het nodig zijn ze aan te passen of te verbeteren om het managen van risico's doelmatig, doeltreffend en consistent te maken.



Figuur 1 — Principes, het raamwerk en het proces

ISO 31000:2018 (N)

Risicomanagement – Richtlijnen

1 Onderwerp en toepassingsgebied

Dit document biedt richtlijnen voor het managen van risico's waarmee organisaties worden geconfronteerd. De toepassing van deze richtlijnen kan voor elke organisatie en de context ervan op maat worden aangepast.

Dit document biedt een generieke benadering voor het managen van alle typen risico's en is niet bedrijfstak- of sectorspecifiek.

Dit document kan worden gebruikt gedurende de gehele levenscyclus van de organisatie en kan worden toegepast op alle activiteiten, met inbegrip van besluitvorming op alle niveaus.

2 Normatieve verwijzingen

Dit document bevat geen normatieve verwijzingen.

3 Termen en definities

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

ISO en IEC onderhouden op de volgende adressen terminologiedatabases voor gebruik in het kader van normalisatie:

— ISO Online browsing platform: te bereiken op http://www.iso.org/obp

— IEC Electropedia: te bereiken op http://www.electropedia.org

3.1
risico
effect van onzekerheid op (het behalen van) doelstellingen

Opmerking 1 bij de term: Een effect is een afwijking van hetgeen verwacht wordt. Dit kan positief, negatief of beide zijn en kan kansen of bedreigingen aanpakken, creëren of daarin resulteren.

Opmerking 2 bij de term: Doelstellingen kunnen verschillende aspecten en categorieën betreffen en kunnen op verschillende niveaus worden toegepast.

Opmerking 3 bij de term: Risico wordt meestal uitgedrukt in termen van *risicobronnen* (3.4), mogelijke *gebeurtenissen* (3.5), alsmede de *gevolgen* (3.6) en de *waarschijnlijkheid* (3.7) ervan.

3.2
risicomanagement
gecoördineerde activiteiten om een organisatie te sturen en te beheersen met betrekking tot *risico's* (3.1)

3.3
belanghebbende
persoon of organisatie die invloed kan uitoefenen op, invloed ondervindt van, of invloed meent te ondervinden van een besluit of activiteit

Opmerking 1 bij de term: De term 'stakeholder' kan als alternatief voor 'belanghebbende' worden gebruikt.