

DIN ISO 31000**DIN**

ICS 03.100.01

Einsprüche bis 2011-05-10

Entwurf**Risikomanagement –
Grundsätze und Leitlinien (ISO 31000:2009)**

Risk management –
Principles and guidelines (ISO 31000:2009)

Management du risque –
Principes et lignes directrices (ISO 31000:2009)

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2011-01-10 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an nasg@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de, sofern dort wiedergegeben;
- oder in Papierform an den Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN, 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 33 Seiten

Normenausschuss Sicherheitstechnische Grundsätze (NASG) im DIN

Inhalt

Seite

Nationales Vorwort	3
Einleitung.....	5
1 Anwendungsbereich	8
2 Begriffe	8
3 Grundsätze	15
4 Risikomanagementrahmen.....	16
4.1 Allgemeines	16
4.2 Mandat und Verpflichtung	17
4.3 Gestaltung des Rahmens für die Behandlung von Risiken	18
4.3.1 Verstehen der Organisation und ihres Zusammenhangs	18
4.3.2 Festlegung der Risikomanagementpolitik	19
4.3.3 Verantwortlichkeit.....	19
4.3.4 Integration in Organisationsprozesse	19
4.3.5 Ressourcen	20
4.3.6 Aufbau von Mechanismen für die interne Kommunikation und Berichterstattung.....	20
4.3.7 Aufbau von Mechanismen für die externe Kommunikation und Berichterstattung.....	20
4.4 Umsetzung des Risikomanagements	21
4.4.1 Umsetzung des Rahmens für die Behandlung von Risiken.....	21
4.4.2 Umsetzung des Risikomanagementprozesses	21
4.5 Überwachung und Überprüfung des Rahmens	21
4.6 Kontinuierliche Verbesserung des Rahmens	21
5 Prozess	22
5.1 Allgemeines.....	22
5.2 Kommunikation und Konsultation	22
5.3 Erstellen des Zusammenhangs.....	23
5.3.1 Allgemeines.....	23
5.3.2 Erstellen des externen Zusammenhangs.....	24
5.3.3 Erstellen des internen Zusammenhangs	24
5.3.4 Erstellen des Zusammenhangs für den Risikomanagementprozess.....	25
5.3.5 Festlegung von Risikokriterien	26
5.4 Risikobeurteilung.....	26
5.4.1 Allgemeines.....	26
5.4.2 Risikoidentifikation.....	26
5.4.3 Risikoanalyse.....	27
5.4.4 Risikobewertung.....	27
5.5 Risikobewältigung	28
5.5.1 Allgemeines.....	28
5.5.2 Auswahl von Maßnahmen zur Risikobewältigung	28
5.5.3 Erstellung und Umsetzung von Risikobewältigungsplänen	29
5.6 Überwachung und Überprüfung.....	29
5.7 Aufzeichnungen über den Risikomanagementprozess.....	30
Anhang A (informativ) Merkmale eines erweiterten Risikomanagements.....	31
A.1 Allgemeines	31
A.2 Wesentliche Ergebnisse	31
A.3 Merkmale	31
A.3.1 Kontinuierliche Verbesserung.....	31
A.3.2 Vollständige Verantwortung für Risiken	31
A.3.3 Anwendung des Risikomanagements in allen Entscheidungen	32
A.3.4 Kontinuierliche Kommunikation	32
A.3.5 Vollständige Integration in die Unternehmensführung der Organisation	32
Literaturhinweise	33

Nationales Vorwort

Das internationale Dokument ISO 31000:2009 ist unverändert in diesen Norm-Entwurf übernommen worden.

Die zugrunde liegende Internationale Norm ISO 31000:2009 wurde von der Arbeitsgruppe "Risk management" (Sekretariat: JISC, Japan) des ISO Technical Management Boards (ISO/TMB) ausgearbeitet.

Die Veröffentlichung der Internationalen Norm ISO 31000:2009 als DIN-ISO-Norm-Entwurf wurde unter der Maßgabe, dass die nationale Bewertung des zuständigen Spiegelgremiums NA 095-04-02 AA „Grundlagen des Risikomanagements“ im Nationalen Vorwort sowie in Nationalen Fußnoten berücksichtigt wird, beschlossen.

Ziel der Veröffentlichung dieses nationalen Norm-Entwurfs ist es, die interessierten Kreise in Deutschland dafür zu sensibilisieren, dass der Einfluss der ISO 31000 bei künftigen Überarbeitungen bestehender risikobezogener Normen, beispielsweise in den Bereichen Sicherheit, Gesundheit und Umweltschutz, hinsichtlich der vorgenannten Aspekte kritisch zu hinterfragen ist.

Der NA 095-04-02 AA sieht sich daher veranlasst das Augenmerk der Leser auf folgende Aspekte zu lenken und deren mögliche Konsequenzen zu bedenken:

a) Risikodefinition

Die in ISO 31000 vorgenommene Definition des Begriffs „Risiko“ ist vom jeweiligen Anwender und seinen spezifischen Problemstellungen zu hinterfragen. Zwar wird der Begriff „Risiko“ in den einzelnen Disziplinen je nach Sachlage und im Alltagsgebrauch unterschiedlich definiert. In vielen Fällen ist jedoch das Verständnis etabliert, dass ein bestimmtes Vorgehen oder ein Ereignis mit der Möglichkeit negativer Konsequenzen verbunden ist. Es gibt allerdings auch die Ansicht, dass risikobehaftete Sachlagen auch positive und/oder negative Auswirkungen haben können. ISO 31000 geht davon aus, dass Risiko „neutral“ zu definieren ist (siehe 2.1, Anmerkung 1: „... in positiver und/oder negativer Hinsicht“) und hat den Anspruch, dass diese Definition und das in ISO 31000 dargelegte Risikomanagement und die –prozesse für alle Tätigkeitsbereiche einer Organisation (Entscheidungen, Prozesse, Projekte, Produkte, Dienstleistungen etc.) in Zukunft angewendet werden sollten. Angesichts der Festlegung anderer ISO-Normen und der nationalen und internationalen Gesetzgebung, dass auf den Gebieten menschlicher Sicherheit, Gesundheitsschutz und Umweltschutz keine Risiken mit „positiven Auswirkungen“ als Grundlage entsprechender Bewertungen und Einschätzungen existieren, ist der in der vorliegenden Norm festgelegte Risikobegriff hinsichtlich der genannten Gebiete vom Anwender dieser Norm stets zu hinterfragen.

b) Risikoabwägung

Bei dem in einzelnen Abschnitten von ISO 31000 vorgeschlagenen Risikomanagement und der Bewertung von Risiken sind Sicherheitsaspekte, der Schutz der menschlichen Gesundheit und der Umweltschutz nicht zwingend zu beachten. Dies liegt zum Beispiel an der Verwendung des Hilfsverbs „kann“. Dies könnte dazu führen, dass bei Risikomanagementprozessen finanzielle Abwägungen (siehe Nationale Fußnote N 10 zu 5.5.2) Vorrang gegenüber Sicherheit, Schutz der menschlichen Gesundheit und der natürlichen Lebensgrundlagen erhalten, da sie gegeneinander abgewogen werden können. Rechtliche Rahmenbedingungen, gesellschaftliche Verantwortung oder der Schutz der Umwelt sollten jedoch Priorität haben und nicht – wie es ISO 31000 an einigen Stellen suggeriert – lediglich Berücksichtigung finden.