

DIN ISO 31000

ICS 03.100.01

Einsprüche bis 2018-06-13

Entwurf

**Risikomanagement –
Leitlinien (ISO 31000:2018);
Text Deutsch und Englisch**

Risk management –
Guidelines (ISO 31000:2018);
Text in German and English

Management du risque –
Lignes directrices (ISO 31000:2018);
Texte en allemand et anglais

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2018-04-13 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

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

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an info@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Organisationsprozesse (NAOrg), 10772 Berlin, 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 44 Seiten

DIN-Normenausschuss Organisationsprozesse (NAOrg)

Inhalt

	Seite
Nationales Vorwort.....	3
Nationaler Anhang NA (informativ) Literaturhinweise	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich.....	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Grundsätze	9
5 Rahmenwerk.....	11
5.1 Allgemeines	11
5.2 Führung und Verpflichtung.....	12
5.3 Integration	13
5.4 Gestaltung.....	13
5.4.1 Verstehen der Organisation und ihres Zusammenhangs	13
5.4.2 Artikulieren der Risikomanagementverpflichtung	14
5.4.3 Zuweisung von organisatorischen Rollen, Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten	14
5.4.4 Zuordnung von Ressourcen	14
5.4.5 Einrichten der Kommunikation und Konsultation	15
5.5 Implementierung.....	15
5.6 Bewertung.....	15
5.7 Verbesserung	16
5.7.1 Anpassen.....	16
5.7.2 Fortlaufendes Verbessern	16
6 Prozess.....	16
6.1 Allgemeines	16
6.2 Kommunikation und Konsultation	17
6.3 Anwendungsbereich, Kontext und Kriterien	17
6.3.1 Allgemeines	17
6.3.2 Festlegen des Anwendungsbereichs.....	18
6.3.3 Externer und interner Kontext.....	18
6.3.4 Festlegen von Risikokriterien.....	18
6.4 Risikobeurteilung.....	19
6.4.1 Allgemeines	19
6.4.2 Risikoidentifikation.....	19
6.4.3 Risikoanalyse	20
6.4.4 Risikobewertung.....	21
6.5 Risikobehandlung	21
6.5.1 Allgemeines	21
6.5.2 Auswahl von Maßnahmen zur Risikobehandlung.....	21
6.5.3 Erstellen und Implementieren von Plänen zur Risikobehandlung.....	22
6.6 Überwachen und Überprüfen.....	23
6.7 Aufzeichnen und Berichten.....	23
Literaturhinweise.....	24

Nationales Vorwort

Dieses Dokument enthält die deutsche Übersetzung der Internationalen Norm ISO 31000:2018, der unter Beteiligung deutscher Experten vom Technischen Komitee ISO/TC 262 „Risk Management“ erarbeitet wurde, dessen Sekretariat von BSI (Vereinigtes Königreich) gehalten wird.

Das internationale Dokument (ISO 31000:2018) ist unverändert in diesen Norm-Entwurf übernommen worden.

Das zuständige deutsche Normungsgremium ist der Arbeitsausschuss NA 175-00-04 AA „Grundlagen des Risikomanagements“ im DIN-Normenausschuss Organisationsprozesse (NAOrg).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Der Veröffentlichung des vorliegenden Norm-Entwurfs liegt der Beschluss 12/2017 des NA 175-00-04 AA zu Grunde, die Internationale Norm ISO 31000:2018 nach deren Erscheinen als DIN ISO-Norm in das DIN-Normenwerk übernehmen zu wollen. Die ISO-Vorgängerausgabe von 2009 war seinerzeit seitens DIN als deutschsprachiger Norm-Entwurf E DIN 31000:2011-01 veröffentlicht und nach Ablauf der zweijährigen Laufzeit des Norm-Entwurfs wegen damals vom zuständigen Spiegelgremium im Nationalen Vorwort und in den Nationalen Fußnoten dargelegter, kritisch zu bewertender Aspekte ersatzlos zurückgezogen worden.

Die vorliegende deutsche Übersetzung der ISO 31000:2018 wurde in Zusammenarbeit mit Experten des zuständigen Spiegelgremiums der Schweizerischen Normenvereinigung (SNV) und unter Mitwirkung des zuständigen Vertreters des Austrian Standards Institute (ASI) erarbeitet.

Nach Auffassung des NA 175-00-04 AA sind mit dem Ergebnis der Revision die seinerzeit von deutscher Seite eingebrachten kritisch bewerteten Aspekte erledigt. Die wesentlichen Ergebnisse der Revision der Norm sind:

- a) Diese Internationale Norm kann für jegliche Art von Risiko von Organisationen angewendet werden, seien die Auswirkungen positiv oder negativ. Somit kann die Norm auch dort angewendet werden, wo ausschließlich positive oder ausschließlich negative Auswirkungen auftreten.
- b) Das Risikomanagement ist auf den internen und externen Kontext ausgerichtet. Dies erfordert eine Anpassung an alle relevanten rechtlichen und regulatorischen Anforderungen sowie an allgemein anerkannte Grundsätze von Sicherheit, Gesundheitsschutz und Umweltschutz.
- c) Die Auswahl der am besten geeigneten Risiko-Behandlungsoption beinhaltet grundsätzlich die Abwägung der Kosten und des Implementierungsaufwands gegen die zu erwartenden Vorteile. Wenn allerdings einige Risiken aus rein ökonomischen Gründen keine Risikobehandlung rechtfertigen, sollte dennoch eine Risikobehandlung erfolgen, insbesondere wenn davon Rechtspflichten oder die Sicherheit, der Gesundheitsschutz oder der Umweltschutz betroffen sind. Des Weiteren wird, unabhängig von der Höhe der Kosten, die Betrachtung von Risiken nicht ausgeschlossen, deren Auswirkungen hoch und somit von besonderer Bedeutung sind.

Mit der Revision ist unter Beibehaltung der Gesamtstruktur eine kürzere Norm mit klarerem Wortlaut entstanden, so dass weiterhin generische Empfehlungen zum Risikomanagement für Organisationen aller Art und Größenordnung und für jede Risikoart zur Verfügung stehen. Die Norm ist damit zugleich der Maßstab für Managementsystemnormen der ISO, deren Ansatz aufgrund der Vorgaben der ISO auf dem Risikomanagement aufbauen muss, ohne selbst eine Managementsystemnorm zu sein. Da die ISO 31000

Empfehlungen liefert, die an die spezifische Organisation angepasst werden können oder müssen, und keine Anforderungen vorgibt, ist weiterhin kein Raum für eine Zertifizierung nach dieser Norm gegeben.

Während die Abschnitte zum Risikomanagement-Rahmenwerk und zum Prozess im Wesentlichen im Wortlaut aktualisiert und noch besser aufeinander abgestimmt wurden, wurden der Anwendungsbereich, die Begriffe sowie der Abschnitt zu den Grundsätzen gründlich überarbeitet und dabei gekürzt. Der Anwendungsbereich wurde auf das Notwendigste beschränkt und enthält damit nicht mehr das in Deutschland kritisch bewertete Primat der Norm im Verhältnis zu Normen, die spezifische Risiken behandeln. Die in der Norm festgelegte Terminologie wurde von ursprünglich 29 auf die acht wesentlichen Begriffe zusammengestrichen. Die Definition von „Risiko“ wurde beibehalten, die Anmerkungen dazu jedoch so überarbeitet, dass nunmehr klargestellt ist, dass auf bestimmten Gebieten (z. B. in der Sicherheitstechnik) ausschließlich negative Auswirkungen vorkommen können. Die Überarbeitung der Grundsätze resultierte in einer Umstrukturierung und Zusammenfassung, so dass nunmehr acht Grundsätze um die Wertschöpfung und -erhaltung als dem Gesamtzweck des Risikomanagements gruppiert wurden (siehe hierzu auch das neue Bild 2).

Im Übrigen legt die Norm besonderes Gewicht auf die Aufgaben der Leitung und die Verpflichtung sowie auf die Integration von Risikomanagement in alle Aktivitäten der Organisation. Die iterative Dynamik der einzelnen Teile des Risikomanagements, wodurch unter Umständen bereits „erledigte Schritte“ bei einer Änderung der Rahmenbedingungen oder Erkenntnisse erneut durchlaufen werden müssen, wird besonders hervorgehoben.

Der Begriff „risk treatment“ wird in dieser Norm entsprechend dessen lexikalischer Bedeutung und in Übereinstimmung mit DIN EN 31010 mit „Risikobehandlung“ übersetzt. Darüber hinaus reflektiert der Begriff „Risikobehandlung“, dass Risiken nach dem Verständnis dieser Norm nicht nur mit Bedrohungen, sondern auch mit positiv konnotierten Möglichkeiten („Chancen“) verbunden sind. Letztere werden nicht „bewältigt“, sondern genutzt, was beides vom Oberbegriff „behandeln“ korrekt abgedeckt wird.

Für die in diesem Dokument zitierten internationalen Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 31010

siehe DIN EN 31010

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN 31010, *Risikomanagement — Verfahren zur Risikobeurteilung*

Vorwort

ISO (die Internationale Organisation für Normung) ist eine weltweite Vereinigung nationaler Normungsorganisationen (ISO-Mitgliedsorganisationen). Die Erstellung von Internationalen Normen wird üblicherweise von Technischen Komitees von ISO durchgeführt. Jede Mitgliedsorganisation, die Interesse an einem Thema hat, für welches ein Technisches Komitee gegründet wurde, hat das Recht, in diesem Komitee vertreten zu sein. Internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO stehen, nehmen ebenfalls an der Arbeit teil. ISO arbeitet bei allen elektrotechnischen Themen eng mit der Internationalen Elektrotechnischen Kommission (IEC) zusammen.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Es sollten insbesondere die unterschiedlichen Annahmekriterien für die verschiedenen ISO-Dokumentenarten beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Eine Erläuterung zum freiwilligen Charakter von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO) hinsichtlich technischer Handelshemmnisse (TBT) berücksichtigt, enthält der folgende Link: www.iso.org/iso/foreword.html.

Dieses Dokument wurde vom Technischen Komitee ISO/TC 262 *Risk Management* erarbeitet.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO 31000:2009), die technisch überarbeitet wurde.

Die wesentlichen Änderungen im Vergleich zur Vorgängerausgabe sind folgende:

- Überprüfung der Grundsätze des Risikomanagements, welche die wichtigsten Kriterien für dessen Erfolg sind;
- Hervorhebung der Führung durch die oberste Leitung und der Integration des Risikomanagements, beginnend mit der Leitung der Organisation;
- stärkere Betonung des iterativen Charakters des Risikomanagements, wobei darauf hingewiesen wird, dass neue Erfahrungen, Kenntnisse und Analysen in jeder Phase des Prozesses zu einer Überarbeitung der Prozesselemente, Aktionen und Steuerungen führen können;
- Straffung des Inhalts mit stärkerem Fokus auf die Aufrechterhaltung eines offenen Systemmodells, das mehreren Bedürfnissen und Kontexten gerecht wird.

Einleitung

Dieses Dokument richtet sich an Personen, die Werte in Organisationen schaffen und bewahren, indem sie mit Risiken umgehen, Entscheidungen treffen, Ziele festlegen und erreichen sowie Leistung verbessern.

Organisationen jeglicher Art und Größe unterliegen externen und internen Faktoren und Einflüssen, die das Erreichen ihrer Ziele ungewiss machen können.

Das Umgehen mit Risiken erfolgt iterativ und unterstützt Organisationen dabei, Strategien festzulegen, Ziele zu erreichen und fundierte Entscheidungen zu treffen.

Das Umgehen mit Risiken ist Teil der Leitung und Führung und entscheidet darüber, wie diese Organisation auf allen Ebenen geführt wird. Es trägt zu der Verbesserung von Managementsystemen bei.

Das Umgehen mit Risiken ist Teil aller Aktivitäten einer Organisation und umfasst die Interaktion mit Stakeholdern.

Das Umgehen mit Risiken berücksichtigt den externen und internen Kontext der Organisation einschließlich menschlichen Verhaltens und kultureller Faktoren.

Das Umgehen mit Risiken basiert auf den Grundsätzen dem Rahmenwerk und dem Prozess, wie sie in diesem Dokument beschrieben und in Bild 1 dargestellt sind. Diese Komponenten bestehen möglicherweise bereits vollständig oder teilweise in der Organisation, müssten aber möglicherweise angepasst oder verbessert werden, damit das Umgehen mit Risiken effizient, wirksam und konsistent erfolgt.

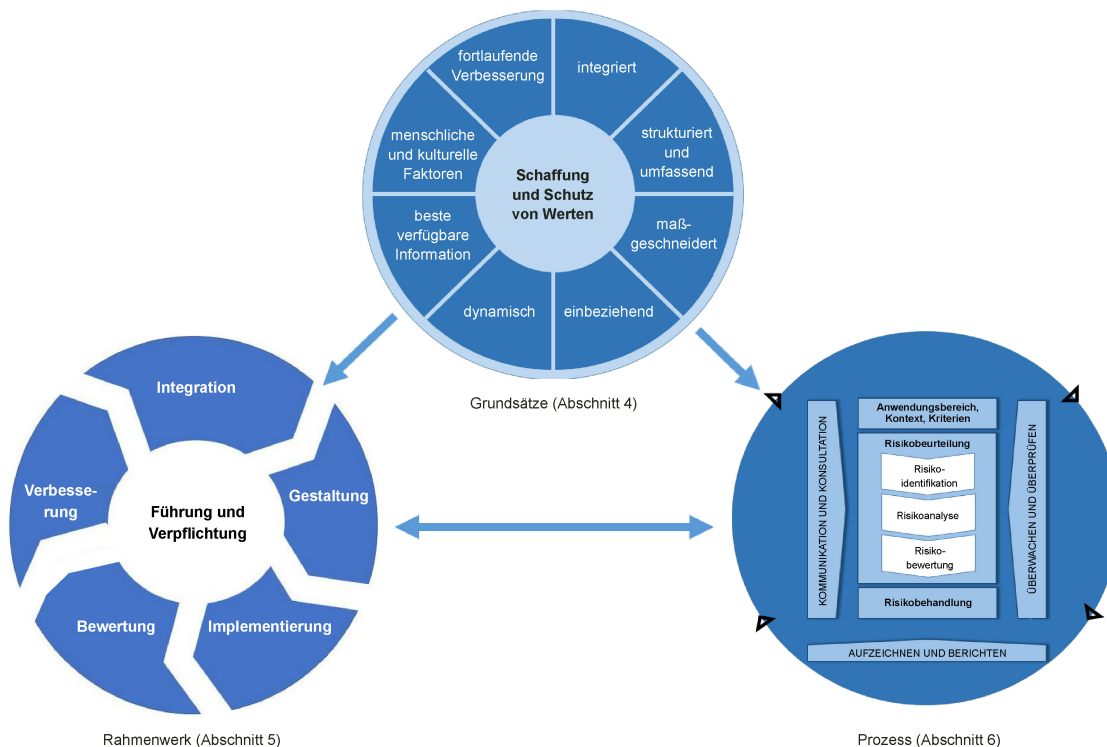


Bild 1 —Grundsätze, Rahmenwerk und Prozess

1 Anwendungsbereich

Dieses Dokument legt Leitlinien für das Umgehen mit Risiken fest, denen Organisationen ausgesetzt sind. Die Anwendung dieser Leitlinien kann an jede Organisation und deren Kontext angepasst werden.

Dieses Dokument bietet einen allgemeinen Ansatz für das Umgehen mit jeglicher Art von Risiko und ist nicht industrie- oder sektorspezifisch.

Dieses Dokument kann während der gesamten Lebensdauer der Organisation genutzt und auf alle Aktivitäten einschließlich der Entscheidungsfindung auf allen Ebenen angewendet werden.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- ISO Online Browsing Platform: unter <http://www.iso.org/obp>
- IEC Electropedia: unter <http://www.electropedia.org>

3.1

Risiko

(en: risk)

Auswirkung von Unsicherheit auf Ziele

Anmerkung 1 zum Begriff: Eine Auswirkung stellt eine Abweichung vom Erwarteten dar. Diese Abweichung kann positiv, negativ oder beides sein und kann auf Möglichkeiten und Bedrohungen eingehen, diese verursachen oder durch diese verursacht sein.

Anmerkung 2 zum Begriff: Ziele können verschiedene Aspekte und Kategorien umfassen und auf allen Ebenen angewendet werden.

Anmerkung 3 zum Begriff: Das Risiko wird üblicherweise anhand der *Risikoursachen* (3.4), der *potenziellen Ereignisse* (3.5), ihrer *Auswirkungen* (3.6) und ihrer *Wahrscheinlichkeit* (3.7) dargestellt.

3.2

Risikomanagement

(en: risk management)

koordinierte Aktivitäten zur Lenkung und Steuerung einer Organisation in Bezug auf *Risiken* (3.1)

3.3

Stakeholder

(en: stakeholder)

Person oder Organisation, die eine Entscheidung oder Aktivität beeinflussen kann, von dieser beeinflusst werden kann oder den Eindruck haben kann, davon beeinflusst zu werden

Anmerkung 1 zum Begriff: Der Begriff „interessierter Kreis“^{N1)} kann alternativ zu „Stakeholder“ verwendet werden.

3.4

Risikoquelle

(en: risk source)

Risikoursache

Element, das alleine oder gemeinsam mit anderen Faktoren potenziell zu *Risiken* (3.1) führt

3.5

Ereignis

(en: event)

Eintritt oder Veränderung einer bestimmten Kombination von Umständen

Anmerkung 1 zum Begriff: Ein Ereignis kann einmal oder mehrmals eintreten und mehrere Ursachen und mehrere *Auswirkungen* (3.6) haben.

Anmerkung 2 zum Begriff: Ein Ereignis kann auch etwas sein, das erwartet wird und nicht eintritt oder etwas, das unerwartet eintritt.

Anmerkung 3 zum Begriff: Ein Ereignis kann eine Risikoquelle sein.

3.6

Auswirkung

(en: consequence)

Ergebnis eines *Ereignisses* (3.5), welches die Ziele betrifft

Anmerkung 1 zum Begriff: Eine Auswirkung kann gewiss oder ungewiss sein und sich direkt oder indirekt bzw. positiv oder negativ auf Ziele auswirken.

Anmerkung 2 zum Begriff: Auswirkungen können qualitativ oder quantitativ beschrieben werden.

Anmerkung 3 zum Begriff: Jede Auswirkung kann durch kaskadierende und kumulative Effekte eskalieren.

3.7

Wahrscheinlichkeit

(en: likelihood)

Möglichkeit, dass etwas geschieht

Anmerkung 1 zum Begriff: In der Terminologie des *Risikomanagements* (3.2) bezeichnet der Begriff „Wahrscheinlichkeit“ die Möglichkeit, dass etwas geschieht, gleichgültig ob diese Möglichkeit objektiv oder subjektiv, qualitativ oder quantitativ definiert, gemessen oder bestimmt und mit allgemeinen Begriffen oder mathematisch (z. B. durch die statistische Wahrscheinlichkeit oder die Häufigkeit in einem bestimmten Zeitraum) beschrieben wird.

Anmerkung 2 zum Begriff: Der englische Begriff „likelihood“ hat in einigen Sprachen keine direkte Entsprechung, wo für „likelihood“ (subjektive Wahrscheinlichkeit) und „probability“ (objektive, mathematische Wahrscheinlichkeit) oft ein und dasselbe Wort verwendet wird. In der englischen Sprache ist der Begriff „probability“ jedoch oftmals sehr eng als mathematischer Begriff definiert. Deshalb wird in der englischen Terminologie des Risikomanagements der Begriff „likelihood“ mit der Absicht verwendet, dass er dieselbe weit gefasste Bedeutung haben sollte wie der Begriff „Wahrscheinlichkeit“ in vielen anderen Sprachen.

N1) Nationale Fußnote: Für den Begriff „interessierter Kreis“ wird als Synonym auch der Begriff „interessierte Partei“ (en: interested party) verwendet.

3.8

Steuerung

(en: control)

Maßnahme, die das *Risiko* (3.1) aufrechterhält und/oder verändert

Anmerkung 1 zum Begriff: Steuerungen umfassen unter anderem alle Prozesse, Grundsätze, Instrumente, Verfahren oder andere Bedingungen und/oder Aktionen, welche Risiken aufrechterhalten oder verändern.

Anmerkung 2 zum Begriff: Steuerungen können nicht immer die beabsichtigte oder angenommene verändernde Wirkung ausüben.

4 Grundsätze

Der Zweck des Risikomanagements besteht darin, Werte zu schaffen und zu bewahren. Es verbessert die Leistung, regt Innovationen an und unterstützt das Erreichen von Zielen.

Die in Bild 2 dargestellten Grundsätze bieten eine Anleitung zu den Eigenschaften eines wirksamen und effizienten Risikomanagements, vermitteln dessen Wert und erläutern dessen Absicht und Zweck. Diese Grundsätze bilden die Grundlage für das Umgehen mit Risiken und sollten bei der Entwicklung des Rahmenwerks und der Prozesse für das Risikomanagement berücksichtigt werden. Diese Grundsätze sollten es einer Organisation ermöglichen, die Auswirkungen von Unsicherheit auf deren Ziele zu behandeln.



Bild 2 — Grundsätze

Ein effektives Risikomanagement erfordert die Grundsätze von Bild 2 und kann wie folgt näher erläutert werden.

a) integriert

Das Risikomanagement ist ein integraler Bestandteil aller Aktivitäten einer Organisation.

b) strukturiert und umfassend

Ein strukturierter und umfassender Risikomanagementansatz trägt zu konsistenten und vergleichbaren Ergebnissen bei.

c) maßgeschneidert

Das Rahmenwerk und die Prozesse des Risikomanagements sind an den externen und internen Kontext einer Organisation angepasst und diesem angemessen sowie mit den Zielen der Organisation verbunden.

d) einbeziehend

Die angemessene und rechtzeitige Beteiligung von Stakeholdern ermöglicht die Berücksichtigung ihrer Kenntnisse, Ansichten und Wahrnehmungen. Dies führt zu verbesserter Erkenntnis und einem fundierten Risikomanagement.

e) dynamisch

Risiken können auftreten, sich verändern oder verschwinden, wenn sich der externe und interne Kontext einer Organisation verändert. Diese Veränderungen und Ereignisse werden durch das Risikomanagement in angemessener Weise und rechtzeitig vorhergesehen, erkannt, bestätigt und behandelt.

f) beste verfügbare Information

Die Eingaben in das Risikomanagement basieren auf historischen und aktuellen Informationen sowie zukünftigen Erwartungen. Das Risikomanagement berücksichtigt ausdrücklich alle Einschränkungen und Unsicherheiten, die mit solchen Informationen und Erwartungen verbunden sind. Informationen sollten zeitgerecht, verständlich und den relevanten Stakeholdern verfügbar sein.

g) menschliche und kulturelle Faktoren

Menschliches Verhalten und Kultur haben einen wesentlichen Einfluss auf alle Aspekte des Risikomanagements auf allen Ebenen und in jeder Phase.

h) fortlaufende Verbesserung

Das Risikomanagement wird durch Lernen und Erfahrung fortlaufend verbessert.

5 Rahmenwerk

5.1 Allgemeines

Der Zweck des Risikomanagement-Rahmenwerks besteht darin, die Organisation dabei zu unterstützen, das Risikomanagement in deren bedeutende Aktivitäten und Funktionen zu integrieren. Die Wirksamkeit des Risikomanagements wird von dessen Integration in die Leitung der Organisation einschließlich der Entscheidungsfindung abhängen. Dies erfordert die Unterstützung durch die Stakeholder, insbesondere durch die oberste Leitung.

Die Entwicklung des Rahmenwerks umfasst das Integrieren, Gestalten, Implementieren, Bewerten und Verbessern des Risikomanagements in der gesamten Organisation. Bild 3 zeigt die Komponenten eines Rahmenwerks.



Bild 3 —Rahmenwerk

Die Organisation sollte ihre bestehenden Risikomanagementverfahren und -prozesse sowie alle Lücken im Rahmenwerk bewerten und behandeln.

Die Komponenten des Rahmenwerks und die Art und Weise, in der diese ineinander greifen, sollten an die Bedürfnisse der Organisation angepasst werden.

5.2 Führung und Verpflichtung

Die oberste Leitung und, wo angezeigt, die Aufsichtsorgane, sollten sicherstellen, dass das Risikomanagement in alle Aktivitäten der Organisation integriert wird, und sollten Führung und Verpflichtung nachweisen durch:

- Anpassen und Implementieren aller Komponenten des Rahmenwerks;
- Veröffentlichen einer Erklärung oder eines Grundsatzdokuments, die einen Risikomanagementansatz, einen Plan oder eine Aktion festlegen;
- Sicherstellen, dass für das Umgehen mit Risiken die erforderlichen Ressourcen bereitgestellt werden;
- Zuweisen von Befugnis, Verantwortlichkeit und Rechenschaftspflicht auf geeigneten Ebenen in der Organisation;;

Dies wird der Organisation helfen, um

- das Risikomanagement auf deren Ziele, Strategie und Kultur abzustimmen;
- alle Verpflichtungen einschließlich ihrer freiwilligen Zusagen zu erkennen und zu behandeln;
- den Grad und die Art des eventuell von dem Unternehmen eingegangenen Risikos zu bestimmen, um die Entwicklung der Risikokriterien zu steuern und sicherzustellen, dass diese der Organisation und deren Stakeholdern mitgeteilt werden;
- den Wert des Risikomanagements der Organisation und ihren Stakeholdern mitzuteilen;
- die systematische Überwachung der Risiken zu unterstützen;
- sicher zu stellen, dass dasRisikomanagement-Rahmenwerk angemessen zum Kontext der Organisation bleibt.

Die oberste Leitung ist für das Umgehen mit Risiken verantwortlich, während die Aufsichtsorgane für die Überwachung des Risikomanagements verantwortlich sind. Die Aufsichtsorgane sind oftmals verpflichtet oder es wird von ihnen erwartet:

- sicherzustellen, dass Risiken bei der Festlegung der Ziele der Organisation angemessen berücksichtigt werden;
- die wesentlichen Risiken für die Organisation zu verstehen, mit denen diese bei der Verfolgung ihrer Ziele ausgesetzt ist;
- sicherzustellen, dass Systeme zum Umgehen mit solchen Risiken implementiert werden und wirksam funktionieren;
- sicherzustellen, dass solche Risiken im Zusammenhang mit den Zielen der Organisation angemessen sind;
- sicherzustellen, dass Informationen über solche Risiken und deren Behandlung richtig kommuniziert werden.

5.3 Integration

Die Integration des Risikomanagements erfordert das Verständnis der Strukturen und des Kontextes der Organisation. Die Strukturen unterscheiden sich je nach Zweck, Zielen und Komplexität der Organisation. Mit Risiko wird in jedem Teil der Organisationsstruktur umgegangen. Jeder in der Organisation ist für das Umgehen mit Risiken mitverantwortlich.

Die Leitung steuert den Kurs der Organisation, deren externe und interne Beziehungen und die erforderlichen Regeln, Prozesse und Verfahren zum Erreichen ihres Zwecks. Die Vorgaben der Leitung werden durch Managementstrukturen in Strategie und zugehörige Ziele überführt, um das erwünschte Niveau einer nachhaltigen Leistung und langfristigen Entwicklungsfähigkeit zu erreichen. Das Festlegen der Rechenschaftspflicht für das Risikomanagement und der Aufsichtsrollen innerhalb der Organisation sind Kernaufgaben der Leitung der Organisation.

Die Integration des Risikomanagements in eine Organisation ist ein dynamischer und iterativer Prozess und sollte an die Bedürfnisse und die Kultur der Organisation angepasst werden. Das Risikomanagement sollte Teil des Zwecks, der Leitung, der Führung und der Verpflichtung sowie der Strategie, der Ziele und der Abläufe der Organisation und nicht davon getrennt sein.

5.4 Gestaltung

5.4.1 Verstehen der Organisation und ihres Zusammenhangs

Die Organisation sollte beim Gestalten des Rahmenwerks für das Umgehen mit Risiken ihren externen und internen Kontext untersuchen und verstehen.

Die Untersuchung des externen Kontextes einer Organisation kann unter anderem Folgendes enthalten:

- soziale, kulturelle, politische, rechtliche, behördliche, finanzielle, technologische, wirtschaftliche und umweltbezogene Faktoren seien sie internationaler, nationaler, regionaler oder lokaler Art;
- wesentliche Schlüsselfaktoren und Trends, welche die Ziele der Organisation beeinflussen;
- die Beziehungen, Wahrnehmung, Werte, Bedürfnisse und Erwartungen externer Stakeholder;
- vertragliche Beziehungen und Verpflichtungen;
- die Komplexität der Netzwerke und Abhängigkeiten.

Die Untersuchung des internen Zusammenhangs einer Organisation kann unter anderem Folgendes enthalten:

- Vision, Mission und Werte;
- Leitung, Organisationsstruktur, Rollen und Rechenschaftspflichten;
- Strategie, Ziele und Grundsätze;
- Kultur der Organisation;
- von der Organisation übernommene Normen, Leitlinien und Modelle;
- Fähigkeiten im Sinne von Ressourcen und Wissen (z. B. Kapital, Zeit, Menschen, geistiges Eigentum, Prozesse, Systeme und Technologien);
- Daten, Informationssysteme und Informationsflüsse;

- Beziehungen zu internen Stakeholdern unter Berücksichtigung ihrer Wahrnehmungen und Werte;
- vertragliche Beziehungen und Verpflichtungen;
- gegenseitige Abhängigkeiten und Verbindungen.

5.4.2 Artikulieren der Risikomanagementverpflichtung

Die oberste Leitung und, wo angezeigt, die Aufsichtsorgane sollten ihre dauerhafte Verpflichtung zum Risikomanagement nachweisen und artikulieren. Dies kann durch ein Grundsatzdokument, eine Erklärung oder in janderer Form erfolgen, welche die Ziele und die Verpflichtung zum Risikomanagement einer Organisation klar vermittelt. Die Verpflichtung sollte unter anderem Folgendes enthalten:

- Zweck des Umgehens mit Risiken der Organisation und Verbindungen zu deren Zielen und weiteren Grundsätzen;
- Bekräftigen der Notwendigkeit, Risikomanagement in die Gesamtkultur der Organisation zu integrieren;
- Integration des Risikomanagements in die Aktivitäten des Kerngeschäfts und die Entscheidungsfindung leiten;
- Befugnisse, Verantwortlichkeiten und Rechenschaftspflichten;
- Bereitstellung der notwendigen Ressourcen;
- Vorgehensweise bei der Handhabung widersprüchlicher Ziele;
- Messung und Berichterstattung innerhalb der Leistungsindikatoren der Organisation;
- Überprüfung und Verbesserung.

Soweit angemessen, sollte die Verpflichtung zum Risikomanagement innerhalb einer Organisation und zu Stakeholdern kommuniziert werden.

5.4.3 Zuweisung von organisatorischen Rollen, Befugnissen, Verantwortlichkeiten und Rechenschaftspflichten

Die oberste Leitung und, wo angezeigt, die Aufsichtsorgane sollten sicherstellen, dass die Befugnisse, Verantwortlichkeiten und Rechenschaftspflichten für die relevanten Rollen in Bezug auf das Risikomanagement zugewiesen und auf alle Ebenen der Organisation kommuniziert werden, und sollten

- betonen, dass das Risikomanagement eine Hauptverantwortlichkeit ist,
- die Personen mit Rechenschaftspflicht und Befugnis für das Umgehen mit Risiko (Risikoeigner) bestimmen.

5.4.4 Zuordnung von Ressourcen

Die oberste Leitung und, wo angezeigt, die Aufsichtsorgane sollten die Zuteilung geeigneter Ressourcen für das Risikomanagement sicherstellen, die unter anderem Folgendes umfassen können:

- Personen, Fähigkeiten, Erfahrungen und Kompetenzen;
- Prozesse, Methoden und Werkzeuge der Organisation zum Umgehen mit Risiko;
- dokumentierte Prozesse und Verfahren;