Strategien und Lösungen für integrierte Managementsysteme

TÜV Media

# Chancen nutzen, Risiken überwachen



TÜVRheinland
Genau. Richtig.

**Autor:**

Dr.-Ing. Wolfgang Kallmeyer,
Partner der TÜV Rheinland Consulting GmbH



**Bibliografische Informationen der Deutschen Nationalibliothek**
Die Deutsche Nationalibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-7406-0749-4 (Print)
ISBN 978-3-7406-0750-0 (E-Book)



www.tuev-media.de

## Über die Broschüre

**Motivation**

Risiken gehören zum Alltag für Menschen und Organisationen. Wir versuchen durch vorsichtiges und vorausschauendes Verhalten Gefahren aus dem Weg zu gehen. Dies tun wir meist unbewusst und reflexartig auf der Grundlage von Erfahrungen aus der Vergangenheit, häufig aber auch auf der Basis einer bewussten Planung.

**Risiko und Chance im Managementsystem**

Aus der Technik sind methodische Ansätze zur Risikoidentifikation und Risikovermeidung nicht mehr wegzudenken, sei es für den Betrieb einer Chemieanlage oder die Sicherheit eines Flugzeugs. Die Literatur zum Thema Risikomanagement könnte heute Bibliotheken füllen. Das Thema scheint für uns enorm wichtig zu sein, aber was hat das Ganze mit Managementsystemen zu tun? Die Antwort findet sich bereits in der Qualitätsnorm ISO 9001:2015. Das Erreichen oder Übertreffen eines geplanten Ergebnisses, sei es ein Produkt oder eine Dienstleistung, erfüllt das Kriterium der Qualität. Gelingt es uns nicht, das geplante Ergebnis zu erreichen, haben wir ein realisiertes Risiko, bei einem Produkt sprechen wir dann von Ausschuss oder Nacharbeit. Übertreffen wir das geplante Ergebnis, haben wir eine realisierte Chance. Auf ein Produkt bezogen hieße das, es ist besser als geplant, und wir haben einen Wettbewerbsvorteil auf dem Markt.

**Normforderung**

Weil das Thema Risiko und Chancen so wichtig für den Erfolg einer Organisation ist, ist in die zertifizierbaren ISO-Normen, allen voran die ISO 9001, ein Forderungskapitel zum Umgang mit Risiken und Chancen aufgenommen worden. Seitdem müssen sich Anwender in ihrem jeweils spezifischen Managementsystem mit diesem Thema auseinandersetzen.

In dieser Broschüre erfahren Sie, welche Forderungen aufgrund der Normkapitel 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen“ der ISO-Normen 9001, 14001, 45001 und 50001 für die Organisationen bestehen. Wir erläutern Ihnen, welche Zusammenhänge es dabei mit dem Kontext der Organisation, den Erwartungen interessierter Parteien (Stakeholder) und den Prozessen der Organisation gibt, und wir zeigen ihnen, welche Verbindungen zu rechtlichen Anforderungen bezüglich des Risikomanagements es gibt.

**Ermittlung und Bewertung in der Praxis**

Außerdem erhalten Sie Hinweise, in welchen Schritten und mit welchen Methoden Sie die Ermittlung und Bewertung von Risiken und Chancen in der Praxis gestalten können und welche Freiräume Sie haben, um den Umgang mit Risiken und Chancen normativ korrekt und den Bedürfnissen Ihrer Organisation entsprechend umzusetzen.

Sie erfahren, dass eine ursächliche Verbindung zwischen dem Thema Risiken und Chancen und den Normenforderungen der Normkapitel 4.1 „Verstehen der Organisation“ sowie 4.2 „Verstehen der Erfordernisse und Erwartungen interessierter Parteien“ besteht und wie sich die methodischen Ansätze zur Erfüllung aller drei Normenpunkte mittels Matrixverfahren miteinander verbinden lassen.

Wir zeigen Ihnen auch, warum das Thema Risiken und Chancen in der Organisation ein Thema für die oberste Leitung sind und warum dies wesentlich zur Absicherung des Unternehmenserfolgs beiträgt.

Zudem stellen wir Ihnen mit der Risikomatrix nach Nohl und der Fehler-Möglichkeit-Einfluss-Analyse (FMEA) zwei methodische Ansätze vor, wie Sie eine Risikoerfassung mit einer Risikobewertung und der Risikobehandlung verbinden können.

Dabei unterstützen Sie Arbeitshilfen und Beispiele, um die Bedeutung (Kritikalität) des Kontexts und der Stakeholder für eine Organisation zu ermitteln. Auf diesen Informationen können Sie dann aufbauen und die Risiko- und Chancenbewertung mittels der Nohl-Matrix oder des FMEA-Verfahrens durchführen.

**Arbeitshilfen zum Download**

Die im Text angeführten Klammersymbole verweisen auf diese Arbeitshilfen, die wir Ihnen zum Download bereitgestellt haben. Sie können die Dokumente frei bearbeiten und an Ihre eigenen betrieblichen Anforderungen anpassen.

**IMS-Normforderungen.xlsx**

**Verweismatrix „Normenforderungen an Risiken und Chancen ISO 9001/14001/45001/50001“**

Übereinstimmungen und Unterschiede im IMS

Die vier Normen ISO 9001, 14001, 45001 und 50001 des betrachteten IMS enthalten die Anforderung, sich mit den themenspezifischen Risiken und Chancen der Einzelnormen auseinanderzusetzen. Oberflächlich betrachtet stimmen die Forderung nach einer Risiko- und Chancenbetrachtung grundsätzlich überein. Schaut man in die Detailforderungen, werden normenspezifische Unterschiede an vielen Stellen deutlich. Diese Details der normenspezifischen Unterschiede können Sie der Verweismatrix „Normenforderungen an Risiken und Chancen ISO 9001/14001/45001/50001“ in der beigefügten Arbeitshilfe entnehmen.

**Kontext_Stakeholder_Prozesse.xlsx**

**Übersicht „Beispiele zum Kontext, Stakeholdern und Prozessen: ISO 9001/14001/45001/50001“**

Risiken und Chancen werden vom Kontext, wie z. B. dem Marktumfeld oder dem Ausbildungsgrad der Mitarbeitenden, von den interessierten Parteien (Stakeholder), die sich im Umfeld der Organisation bewegen sowie auch den IMS-Prozessen und ihren Wechselwirkungen selbst beeinflusst. Die Arbeitshilfe „Beispiele zum Kontext, Stakeholdern und Prozessen: ISO 9001/14001/45001/50001“ fasst in den Tabellenblättern „Potenzieller Kontext“, „Potenzielle Stakeholder“ und „Typische Prozesse“ die entsprechenden Aspekte jeweils in einer eigenen Übersichtsmatrix im Vergleich der betrachteten Managementsystemen zusammen.

**Analyse_Bewertung.xlsx**

**Rechentool „Analyse und Bewertung Kontext, Stakeholder und Prozesse – Beispiel“**

Kontext, Stakeholder und Prozesse sind hinsichtlich Risiken und Chancen in ihrer Bedeutung für das Unternehmen zu bewerten. Für die Bewertung dieser Themen bietet es sich an, die Kriterien übersichtlich und nachvollziehbar z. B. in einer Tabelle zu dokumentieren. Die Arbeitshilfe „Analyse und Bewertung Kontext, Stakeholder und Prozesse“ ist mit entsprechenden Beispielen in Form einer Excel-Tabelle beigefügt. Den Themen Kontext, Stakeholder und Prozesse ist jeweils ein Tabellenblatt zugeordnet. Neben der Berechnung des Kritikalitätsfaktors werden zur Bewertung jedes einzelnen Kontexts/Stakeholders/Prozesses sind in der Tabelle noch der Status von bindenden Verpflichtungen eingetragen und ob sich eine Chance, ein Risiko oder ggf. beides ergibt. Diese Informationen werden für eine nachfolgende Risiko- und Chancenbetrachtung als Eingangsinformation benötigt. Die Tabellen können an die eigenen Gegebenheiten für die Bewertung des Unternehmens angepasst und verwendet werden.

**Risiko-Chancen-Bewertung_Nohl.xlsx**

**Rechentool „Risiko-Chancen-Bewertung: Kontext, Stakeholder, Prozesse – Beispiel nach Nohl“**

Die Risikoermittlung und Bewertung nach Nohl betrachtet die Dimensionen Schadensausmaß und Eintrittswahrscheinlichkeit und ist hier in einem an die normative Risikobearbeitung angepassten Tool inkl. einem umfangreichen Beispiel umgesetzt. Darin werden die Aufgabenprioritäten entsprechend Ihrer Eingaben berechnet und farblich zugeordnet. In den unterschiedlichen Ausprägungen der Matrix für „Risiko“ und für „Chancen“ sind zu den Kategorien „Kontext“, „Stakeholder“ und „Prozesse“ jeweils eigene Tabellenblätter angelegt. Sie können das Tool an die Belange in Ihrem Unternehmen anpassen und für die eigene Risiko-Chancen-Bewertung nutzen.

**Rechentool „Risiko-Chancen-Bewertung: Kontext, Stakeholder, Prozesse – Beispiel nach der FMEA-Methode“**

Die Risiko-Chancen-Betrachtung nach der FMEA-Methode ist in ihrer Struktur ebenso wie die Nohl-Methode ein Matrixverfahren. Die methodische Herangehensweise ist jedoch neben der Risikoauswirkung und der Eintrittswahrscheinlichkeit um das dritte Kriterium Entdeckungswahrscheinlichkeit erweitert. Auch für eine Risiko-Chancen-Bewertung nach der FMEA-Methode finden Sie ein bearbeitbares Tool mit Beispielen beigefügt. Sie können es an Ihre eigenen Belange anpassen und nutzen.

**Risiko-Chancen-Bewertung_FMEA.xlsx**

Die Arbeitshilfen stehen für Sie zusammengefasst in einer ZIP-Datei zum Download bereit unter:

**Download**

[redacted]

Passwort: [redacted]

## Inhalt

# 1 Risiken- und Chancenmanagement

## 1.1 Allgemeines

**Erfolg oder Desaster**

Dass bei allem, was wir tun, auch Risiken und Chancen (R&C) mit im Spiel sind, ist für jeden Menschen, aber auch für Organisationen keine neue Erkenntnis. Ob wir Erfolg haben oder nicht, hängt auch davon ab, ob es Einflüsse gibt, die ggf. dazu führen, dass ein vermeintlich guter Plan misslingt oder ein Projekt ein Fehlschlag wird. Es ist eine Frage der Wahrscheinlichkeit, ob ein Ereignis (positiv wie negativ) eintritt, und die genannten Einflüsse lassen sich statistisch beschreiben. Die Prognose, ob das Ereignis zu einem Erfolg oder einem Desaster wird, basiert auf der Bewertung der möglichen Auswirkungen, die dieses Ereignis hervorrufen kann. Überwiegen die Risiken, wird es ein Desaster. Überwiegen die Chancen, wird es ein Erfolg. Der Ausgang eines Vorhabens kann beeinflusst werden, indem Risiken für den Misserfolg minimiert und Chancen für den Erfolg gesteigert werden.

**Zielsetzung**

Dies ist einer der Gründe, warum das Thema Risiken und Chancen ab 2015 mit der Revision der ISO 9001 in die ISO-Managementsystemnormen aufgenommen wurde. Die Normen wollten den Organisationen eine Hilfestellung zu spezifischen Themen wie Qualitäts- oder Umweltmanagement geben, damit diese in diesen Bereichen erfolgreich agieren können. Risiken können diesen Erfolg gefährden, und nicht ergriffene Chancen können den möglichen Erfolg schmälern. Mit dem Einsatz von entsprechenden Methoden und Werkzeugen sollen Risiken frühzeitig erkannt und minimiert sowie Chancen ergriffen werden. Ziel der Normen ist also das Managen, das proaktive Gestalten von Risiken und Chancen durch die Organisation.

**Begriffe Risiko und Chance**

Um mit Begriffen richtig umgehen zu können, muss man sie definieren.

Allgemein sind die Begriffe wie folgt definiert:

**Risiko:** mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis. Möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verluste oder Schäden verbunden sind.

**Chance:** günstige Gelegenheit, Möglichkeit, etwas Bestimmtes zu erreichen, Aussicht auf Erfolg.

Im Leitfaden ISO 9000:2015 „Qualitätsmanagementsysteme – Grundlagen und Begriffe“ steht als Definition [1]

**Risiko:** „Auswirkung von Ungewissheit. Abweichung vom Erwarteten in positiver wie negativer Hinsicht“ (Punkt 3.7.9)

**Chance:** keine eigenständige Definition vorhanden

Die ISO 9001:2015 [2] enthält keine eigene Definition, sondern verweist auf die ISO 9000:2015. Die ISO-Normen 14001:2015 [3], 45001:2018 [4] und 50001:2018 [5] übernehmen die Risikodefinition der ISO 9000. Die ISO 14001 bietet noch eine Definition für den gemeinsamen Begriff „Risiko und Chance“ an: potenziell ungünstige Auswirkung (Bedrohung), potenziell günstige Auswirkung (Chance).

Der Leitfaden DIN ISO 31000:2018 „Risikomanagement – Leitlinien“ [6] erweitert die Definition der ISO 9000:

**Risiko:** Auswirkung von Unsicherheit auf Ziele (wobei die Auswirkung eine positive oder negative Abweichung von der Erwartung ist) (Punkt 3.1)

Damit wird der Begriff Ziele in Verbindung mit Risiken gebracht. Das ist kein Widerspruch, da Ziele nur eine andere Beschreibung von geplanten Ergebnissen oder geplanten Erwartungen sind.

## 1.2 Rechtliche Anforderungen an das Risikomanagement

Die rechtlichen Grundlagen eines unternehmensweiten Risikomanagements sind dem Umstand geschuldet, dass Organisationen und Unternehmen durch unzureichende Kontrolle von wirtschaftlichen Risiken in existenzielle Gefahren geraten können, die Auswirkungen auf die Gesamtwirtschaft oder auf Teile davon haben können. Voraussetzung dafür ist, dass die wirtschaftliche Bedeutung dieser Unternehmen für die Gesamtwirtschaft sehr groß ist, z. B. Banken oder Großkonzerne.

**KonTraG**

Große Firmenzusammenbrüche führten in den 90er-Jahren zu massiver Kritik am praktizierten Risikomanagement in deutschen Firmen. Die Folge war ein Bundesgesetz, das 1998 in Kraft trat, das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) [7], [8]. Das Gesetz schuf einen grundsätzlich neuen Rahmen für die Aufsichtspflicht und das Risikomanagement in großen deutschen Unternehmen. Damit waren erweiterte Pflichten für Vorstände, Geschäftsführer, Wirtschaftsprüfer und Sicherheitsmanager verbunden. Mit dem KonTraG werden zwei grundlegende Regelungsziele verfolgt. Zum einen sollen Schwächen und Verhaltensfehler im Kontrollsystem des deutschen Aktienrechts korrigiert werden, andererseits sollte den deutschen Kapitalgesellschaften der Zugang zu den internationalen Kapitalmärkten erleichtert werden, indem deren Informationsbedürfnis Rechnung getragen wurde.

**Früherkennungssystem für Risiken**

Das KonTraG präzisiert und erweitert hauptsächlich Vorschriften des Handelsgesetzbuchs und des Aktiengesetzes. Kern des KonTraG ist eine Vorschrift, die die Unternehmensleitungen dazu zwingt, ein unternehmensweites Früherkennungssystem für Risiken einzuführen und zu betreiben sowie Aussagen zu Risiken und Risikostrukturen des Unternehmens im Lagebericht des Jahresabschlusses der Gesellschaft zu veröffentlichen. Dazu schreibt das Gesetz in § 91 Abs. 2 AktG die Einrichtung eines Überwachungssystems vor, das den Vorstand verpflichtet, geeignete Maßnahmen zu treffen, damit negative Entwicklungen, die den Fortbestand der Gesellschaft gefährden, frühzeitig erkannt werden können. Solche „bestandsgefährdenden Entwicklungen" ergeben sich meist aus Kombinationseffekten von Einzelrisiken, die in Summe dazu führen, dass eine Gefährdungslage für das Unternehmen eintritt. Aus diesem Grund sind die Unternehmen verpflichtet, regelmäßig eine Risikoanalyse inklusive einer Risikoaggregation durchzuführen.

**Ausstrahlungswirkung**

Das KonTraG betrifft, entgegen weit verbreiteter Meinung, nicht nur Aktiengesellschaften. Auch Kommanditgesellschaften auf Aktienbasis (KGaA) und viele größere Gesellschaften mit beschränkter Haftung (GmbH) fallen darunter – insbesondere dann, wenn in ihnen ein mitbestimmter oder fakultativer Aufsichtsrat existiert, sind diese Gesellschaften von den Vorschriften des KonTraG betroffen (Ausstrahlungswirkung).

Die Rechtsvorschriften des KonTraG haben ihren Ursprung im Aktiengesetz (AktG), im Handelsgesetzbuch (HGB), im Publizitätsgesetz (PublG), im Genossenschaftsgesetz (GenG), sowie im Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG). In ihnen findet man, unabhängig vom KonTraG, in entsprechenden Paragrafen auch Forderungen die zur Erfüllung einen Risikomanagementansatz erfordern.

**Identifikation und Analyse**

Was verlangt der Gesetzgeber im Wesentlichen von den Unternehmen? Er verlangt ein Überwachungssystem zur Früherkennung von bestandsgefährdenden Entwicklungen (im Sinne der Identifikation und Analyse, nicht zur Vermeidung und Reduktion von Risiken) und die Schaffung von angemessenen Strukturen der Kommunikation, die ein frühes Erkennen der Risiken durch die Entscheidungsträger sicherstellen. Auf diese Weise soll rechtzeitig erkannt werden, ob und welche geeigneten Gegenmaßnahmen eingeleitet werden können.

Berichtswesen

Die Ergebnisse des vom KonTraG geforderten Überwachungssystems haben Auswirkungen auf das gesetzlich geforderte Berichtswesen der Unternehmen und auf die Prüfungsberichte der Jahresabschlüsse. Das bedeutet:

- Der Lagebericht zum Jahresabschluss erhält einen höheren Stellenwert mit Prognosecharakter.
- Im Risikolagebericht ist nicht nur auf bestehende Risiken, sondern auch auf Risiken der künftigen Entwicklung einzugehen.
- Die Abschlussprüfer müssen in einem besonderen Teil des Prüfungsberichts
  - dokumentieren, dass und welche Maßnahmen getroffen worden sind,
  - dokumentieren, wie es mit der Effektivität dieser Maßnahmen steht,
  - gesondert auf Risiken eingehen, die den Fortbestand des Unternehmens gefährden können, und
  - dokumentieren, welche Maßnahmen erforderlich sind, um das interne Überwachungssystem zu verbessern.

Wirtschaftsprüfer

Die Wirtschaftsprüfer sind verstärkt zur Risikobeurteilung verpflichtet. Die gesetzlichen Regelungen verpflichten sie und die Geschäftsführung zu einem neuen Risikobewusstsein, das weit über die summarische Prüfung des Lageberichts hinausgeht. In der Konsequenz werden Versäumnisse und Verfehlungen von Aufsichtsrat, Vorstand oder Geschäftsführung, aber auch von Abschlussprüfern vermehrt zu juristischen Haftungsfällen.

Sarbanes-Oxley Act (SOX)

Das KonTraG ist weltweit nicht das einzige Gesetz, das Unternehmen zum Risikomanagement verpflichtet. In den USA gibt es als Bundesgesetz seit 2002 den Sarbanes-Oxley Act (SOX) [9]. Auch er war eine Reaktion des Gesetzgebers auf Bilanzskandale von großen Unternehmen, die den öffentlichen Kapitalmarkt der USA in Anspruch nahmen. Das Gesetz gilt für US-amerikanische und ausländische Unternehmen, deren Wertpapiere an US-Börsen gehandelt werden, deren Wertpapiere mit Eigenkapitalcharakter in den USA außerbörslich gehandelt werden oder deren Wertpapiere in den USA öffentlich angeboten werden, sowie für deren Tochterunternehmen. Das bedeutet, dass auch ausländische Unternehmen unter das Gesetz fallen, wenn sie diese Kriterien erfüllen und in den USA Geschäfte betreiben.

Internes Kontrollsystem (IKS)

Für an US-Börsen notierte Unternehmen bedeutet der Sarbanes-Oxley Act einen erheblichen Eingriff in die unternehmerische Freiheit und die internen Abläufe. Dabei stehen die Regelungen um die Implementierung und Evaluierung eines internen Kontrollsystems (IKS) im Vordergrund. Dieses Kontrollsystem basiert auf den wesentlichen Elementen des Risikomanagements. Es soll vornehmlich die Ordnungsmäßigkeit der Finanzberichterstattung sicherstellen. Nicht zuletzt wegen der erhöhten Haftungsanforderungen an das Management bzgl. der Korrektheit der Finanzberichterstattung rückt die Effektivität des IKS in den Fokus des Managements. Ein gut funktionierendes IKS liegt also im fundamentalen Interesse der Unternehmensführung.

KonTraG und SOX haben hinsichtlich des geforderten Risikomanagements ihren Schwerpunkt bei den finanzwirtschaftlichen Themen. Diese stellen natürlich nicht alle existenzbedrohenden Risiken in einem Unternehmen dar.

EuroSOX

Inzwischen gibt es auch entsprechende Richtlinien der Europäischen Gemeinschaft, die umgangssprachlich unter dem Begriff EuroSOX bekannt sind und vergleichbare Regelungen wie den Sarbanes-Oxley Act enthalten.

Störfallverordnung

Auch im Umweltrecht gibt es Vorgaben, die ein Risikomanagement erfordern. Eine der wichtigen Rechtsvorschriften dazu ist die aus dem Immissionsschutzrecht abgeleitete Störfallverordnung. Nach § 3 „Allgemeine Betreiberpflichten“ (1) hat der Betreiber die nach Art und Ausmaß der möglichen

Gefahren erforderlichen Vorkehrungen zu treffen, um Störfälle zu verhindern. Der Betreiber hat vor Inbetriebnahme ein schriftliches Konzept zur Verhinderung von Störfällen auszuarbeiten und es der zuständigen Behörde auf Verlangen vorzulegen (§ 8 (1)).

**PAAG-Verfahren**

Für Betriebsbereiche der oberen Sicherheitsklasse hat der Betreiber einen Sicherheitsbericht gemäß § 9 zu erstellen, in dem er ein Konzept zur Verhinderung von Störfällen darlegt und nachweist, dass ein Sicherheitsmanagementsystem zu seiner Anwendung vorhanden ist. Grundlage der Risikobeurteilung ist häufig das international anerkannte PAAG-/HAZOP-Verfahren. PAAG [10] steht für

- **P** Prognose (systematische Suche aller möglicher Abweichungen und Störungen),
- **A** Auffinden der Ursachen (Ermitteln der Ursachen innerhalb des untersuchten Systems),
- **A** Abschätzen der Auswirkungen (Ermitteln der logischen Folgen der Abweichung),
- **G** Gegenmaßnahmen (Bewerten vorhandener Maßnahmen und Entscheidung über angemessene weitere Maßnahmen).

**HAZOP-Verfahren**

Vergleichbares leistet das HAZOP-Verfahren (von englisch Hazard and Operability) [11]. Ziel von PAAG/HAZOP ist es, mögliche Abweichungen vom bestimmungsgemäßen Betrieb eines (technischen) Systems aufzudecken, die jeweiligen Ursachen und Auswirkungen zu benennen (und gegebenenfalls zu bewerten) sowie geeignete Maßnahmen zur Verhinderung der Szenarien festzulegen. Darüber hinaus gibt es im Umweltrecht noch weitere Rechtsvorschriften, die zur Verhinderung von Gefahrenlagen ein Risikomanagement zu seiner Bewältigung fordern.

**Arbeitsschutz**

Neben dem Umweltrecht enthält auch das Arbeitsschutzrecht Anforderungen nach Risikomanagementansätzen, um gefährliche Situationen für Menschen zu vermeiden. Gemäß § 3 des Arbeitsschutzgesetzes „Grundpflichten des Arbeitgebers" ist dieser verpflichtet, die erforderlichen Maßnahmen des Arbeitsschutzes unter Berücksichtigung der Umstände zu treffen, die die Sicherheit und Gesundheit der Beschäftigten bei der Arbeit beeinflussen. Dazu gehören auch die nach § 5 durchzuführende Ermittlung der mit der Arbeit verbundenen Gefährdung (Gefährdungs-/Sicherheitsbeurteilung) und die daraus abzuleitende Bewertung, ob Schutzmaßnahmen benötigt werden. Im Fall einer bewerteten Schutznotwendigkeit sind diese zu ergreifen und umzusetzen. Der Arbeitgeber hat die Maßnahmen auf ihre Wirksamkeit zu überprüfen und erforderlichenfalls an sich ändernde Gegebenheiten anzupassen. Die Risikobeurteilung erfolgt häufig gemäß der Risikomatrix nach Nohl.

**ALARP-Verfahren**

Im englischen Sprachraum ist als vergleichbare Methode das ALARP-Verfahren (as low as reasonably practicable) bekannt. Das ALARP-Verfahren besagt, dass Risiken auf ein Maß reduziert werden sollen, das den höchsten Grad an Sicherheit garantiert, der vernünftigerweise praktikabel ist (d. h. finanziell und/oder technisch mit vertretbarem Aufwand realisierbar ist).

**Lieferkettensorgfaltsgesetz**

Überall dort, wo durch Handlungen oder die Nutzung von Produkten/Equipment Gefahren auftreten können, die Leib und Leben und andere Schutzgüter (z. B. Umwelt, Sachgüter, Fauna und Flora) bedrohen, ist auch die Forderung nach einem vorbeugenden Risikoansatz nicht weit. Aber nicht nur Produkte erzeugen für Unternehmen die Pflicht, Verantwortung im Sinne der Risikoabwägung zu übernehmen, sondern der Gesetzgeber erweitert den risikobasierten Ansatz über das eigene Unternehmen hinaus. Das neue Lieferkettensorgfaltsgesetz verpflichtet die größeren Unternehmen in Deutschland, den Schutz von Menschenrechten, Umwelt sowie Sicherheit und Gesundheit

in der eigenen Lieferkette abgestuft (unmittelbar und mittelbar) abzusichern. Daraus ergibt sich die Pflicht zum Risikomanagement, um nachteilige Auswirkungen bei Menschenrechten, Sicherheitsstandards etc. in der Lieferkette zu erkennen und ein Vorgehen zur Behandlung der potenziellen Gefährdungen zu etablieren.

### 1.3 Normative Anforderungen zum Risiko- und Chancenmanagement

**Übereinstimmungen und Unterschiede im IMS**

Alle vier Normen des betrachteten IMS (ISO 9001, 14001, 45001 und 50001) enthalten die Anforderung, sich mit den themenspezifischen Risiken und Chancen der Einzelnormen auseinanderzusetzen. Betrachtet man die einzelnen Normen ISO 9001, 14001, 45001 und 50001, so zeigt sich im Normkapitel 6.1/6.1.1 nur auf den ersten Blick in Bezug auf die Forderung nach einer Risiko- und Chancenbetrachtung eine grundsätzliche Übereinstimmung. Schaut man in die Detailforderungen, werden normenspezifische Unterschiede an vielen Stellen deutlich.

**IMS_ Normenforderungen.xlsx**

Die Details der normenspezifischen Unterschiede können Sie der Verweismatrix „Normenforderungen an Risiken und Chancen ISO 9001/14001/45001/50001" in der beigefügten Arbeitshilfe entnehmen

Hinsichtlich der Integration der Forderungen in einen zentralen Risiko-Chancen-Prozess stellen sich somit Hürden in den Weg, die sicher nicht hilfreich im Sinne eines IMS sind. Da hat die ISO bezüglich der Anwenderfreundlichkeit noch ein Stück Harmonisierungsarbeit vor sich.

**Grundlage eines risikobasierten Denkens**

Die Grundlage eines risikobasierten Denkens als Voraussetzung für das Risikomanagement ist nur in der ISO 9001:2015 verankert. Eine Kernaufgabe für jedes Managementsystem ist, als vorbeugendes Instrument gegen Unwägbarkeiten zu wirken. Das bedeutet, Risiken und Chancen bei der Planung und Verwirklichung der spezifischen Systeme schon am Anfang zu berücksichtigen. Dabei sind folgende Fragen hinsichtlich Risiken und Chancen zu stellen:

- Woher kommen sie, was sind ihre Quellen?
- Wie soll man mit ihnen umgehen, welche Regelungen sind dazu nötig?
- Wie kann das nachvollziehbar gestaltet werden?
- Welche Verantwortlichkeiten müssen dafür geregelt werden?

Der Grundsatz des risikobasierten Denkens oder besser gesagt des risikobasierten Ansatzes (der ISO 9001) in Managementsystemen sollte auf das gesamte IMS Anwendung finden, zum einen aus praktischen Gründen und zum anderen, um den Gedanken der Integration der Systeme konsequent umzusetzen.

**Vergleichbare Anforderungen**

Beginnen wir bei unserer Analyse mit den vergleichbaren Forderungen. Nach Normkapitel 6.1 „Maßnahmen zum Umgang mit Risiken und Chancen" (ISO 9001, 50001) oder 6.1.1 „Allgemeines" (ISO 14001, 45001) sind bei der Planung für die Managementsysteme der Kontext der Organisation (Normkapitel 4.1) und die interessierten Kreise (Normkapitel 4.2) in allen Managementsystemen zu berücksichtigen. Die Verbindung in den Normen zeigt Tabelle 1.

Tabelle 1: Vergleichbare Anforderungen nach Normkapitel 4.1/4.2 im IMS

| Norm | Zu berücksichtigende Anforderungen nach Normkapitel 4.1 und 4.2 |
|---|---|
| ISO 9001 | Risiken und Chancen im QMS berücksichtigen, um<br>• gewünschte Ergebnisse sicherzustellen,<br>• erwünschte Auswirkungen (Chancen) zu verstärken und<br>• unerwünschte Auswirkungen (Risiko) zu verhindern oder zu verringern.<br>Gewünschte Ergebnisse des QMS sind: die Lieferung konformer Produkte und Dienstleistungen, die Erhöhung der Kundenzufriedenheit und die Verbesserung des QM-Systems.<br>Die gewünschten Ergebnisse des QMS werden in der Regel mittels definierter Prozesse umgesetzt. |
| ISO 14001 | Risiken und Chancen im UMS bestimmen, um<br>• sicherzustellen, dass die beabsichtigten Ergebnisse erreicht werden,<br>• unerwünschte Auswirkungen zu verhindern oder zu verringern (unter Berücksichtigung beeinflussender externer Umweltauswirkungen),<br>• fortlaufende Verbesserung zu erreichen.<br>Beabsichtigte Ergebnisse des UMS sind: die Verbesserung der Umweltleistung der Organisation, die Vermeidung von Nichtcompliance sowie die Vermeidung oder Verringerung von Umweltbeeinträchtigungen (z. B. Umweltunfälle).<br>Auch im UMS erfolgt die Umsetzung der beabsichtigten Ergebnisse über definierte Prozesse. |
| ISO 45001 | Risiken und Chancen im SGA-MS bestimmen, um<br>• sicherzustellen, dass die beabsichtigten Ergebnisse erreicht werden,<br>• unerwünschte Auswirkungen zu verhindern oder verringern,<br>• fortlaufende Verbesserung zu erreichen.<br>Beabsichtigte Ergebnisse im SGA-MS sind: fortlaufende Verbesserung der SGA-Leistung, Erfüllung rechtlicher Verpflichtung und anderer Anforderungen sowie das Erreichen von SGA-Zielen.<br>Auch im SGA-MS erfolgt die Umsetzung der beabsichtigten Ergebnisse über definierte Prozesse. |
| ISO 50001 | Risiken und Chancen im EnMS bestimmen, um<br>• das Erreichen der beabsichtigten Ergebnisse sicherzustellen,<br>• unerwünschte Auswirkungen zu verhindern oder zu verringern,<br>• eine fortlaufende Verbesserung des EnMS zu erreichen.<br>Beabsichtigte Ergebnisse des EnMS sind die Verbesserung der energiebezogenen Leistung, die Einhaltung von Compliance und anderer Anforderungen sowie die Energieeffizienz von Prozessen und Einrichtungen.<br>Auch im EnMS erfolgt die Umsetzung der beabsichtigten Ergebnisse über definierte Prozesse. |



**Gemeinsamkeiten**

Die Anforderung für eine Risiko- und Chancenbetrachtung haben alle Managementsysteme des IMS gemeinsam, wenn es um

- das Erreichen der beabsichtigten Ergebnisse der spezifischen Managementsysteme,
- die Förderung erwünschter Auswirkungen und die Verhinderung unerwünschter Auswirkungen,
- sowie um die fortlaufende Verbesserung der spezifischen Managementsysteme und somit auch des gesamten IMS geht.

Damit ist die Anwendung der Forderung nach einer Risiko- und Chancenbetrachtung explizit auf die drei genannten Themenfelder begrenzt. Der wesentliche Unterschied besteht in den erwarteten Ergebnissen, die bei den spezifischen Einzelsystemen naturgemäß andere sind. Das Erreichen der beabsichtigten Ergebnisse der vier spezifischen Managementsysteme ist der wichtigste der drei Punkte.

**Anwendungsbereiche in ISO 14001 und ISO 45001**

Zwei Managementsysteme, die ISO 14001 und die ISO 45001, fordern zusätzlich noch eine Berücksichtigung des Anwendungsbereichs bei der Risiko- und Chancenbetrachtung. Dazu ist vorab die Frage zu klären, was der Anwendungsbereich eines Managementsystems umfasst und wie er definiert ist. Die ISO 14001 liefert im Normkapitel 4.3 „Festlegen des Anwendungsbe-

# TÜV-Media-Fachbroschüren

Wolfgang Kallmeyer
**Integrierte Managementsysteme richtig führen**
76 Seiten / 41,73 EUR / Bestell-Nr. 60689

Wolfgang Kallmeyer
**Der Auditfragenkatalog zur ISO/IEC 27001**
Fragen finden und im internen Audit richtig einsetzen
40 Seiten / 51,36 EUR / Bestell-Nr. 60708

Walter Schlegel / Stefan Pawils
**Die ISO 37301:2021**
Interpretation der Anforderungen
36 Seiten / 39,90 EUR / Bestell-Nr. 60642

Wolfgang Kallmeyer
**Das integrierte Management-Review**
Richtig planen, durchführen, dokumentieren
44 Seiten / 39,90 EUR / Bestell-Nr. 60626

Wolfgang Kallmeyer
**Integrierte Managementsysteme**
Schritte zum nachhaltigen Erfolg
64 Seiten / 39,90 EUR / Bestell-Nr. 60553

Jürgen Ohligschläger
**Die ISO 9001:2015**
Interpretation der Anforderungen
52 Seiten / 39,90 EUR / Bestell-Nr. 60507

Wolfgang Kallmeyer
**Der Auditfragenkatalog zur ISO 9001**
Fragen finden und im internen Audit richtig einsetzen
68 Seiten / 39,90 EUR / Bestell-Nr. 60443

Wolfgang Kallmeyer
**Das Lieferantenaudit**
Erfolgreich vorbereiten und durchführen
74 Seiten / 39,90 EUR / Bestell-Nr. 60407



*Ab einer Bestellmenge von 5 Exemplaren bieten wir Ihnen attraktive Mengenpreise.*

Bestellungen bei TÜV Media:

Telefon: +49 221 806 3511
Telefax: +49 221 806 3510
Webshop: www.tuev-media.de

Alle TÜV Media Fachbroschüren erhalten Sie auch als E-Books unter:
**www.tuev-media.de/ebooks**

TÜVRheinland®
Genau. Richtig.