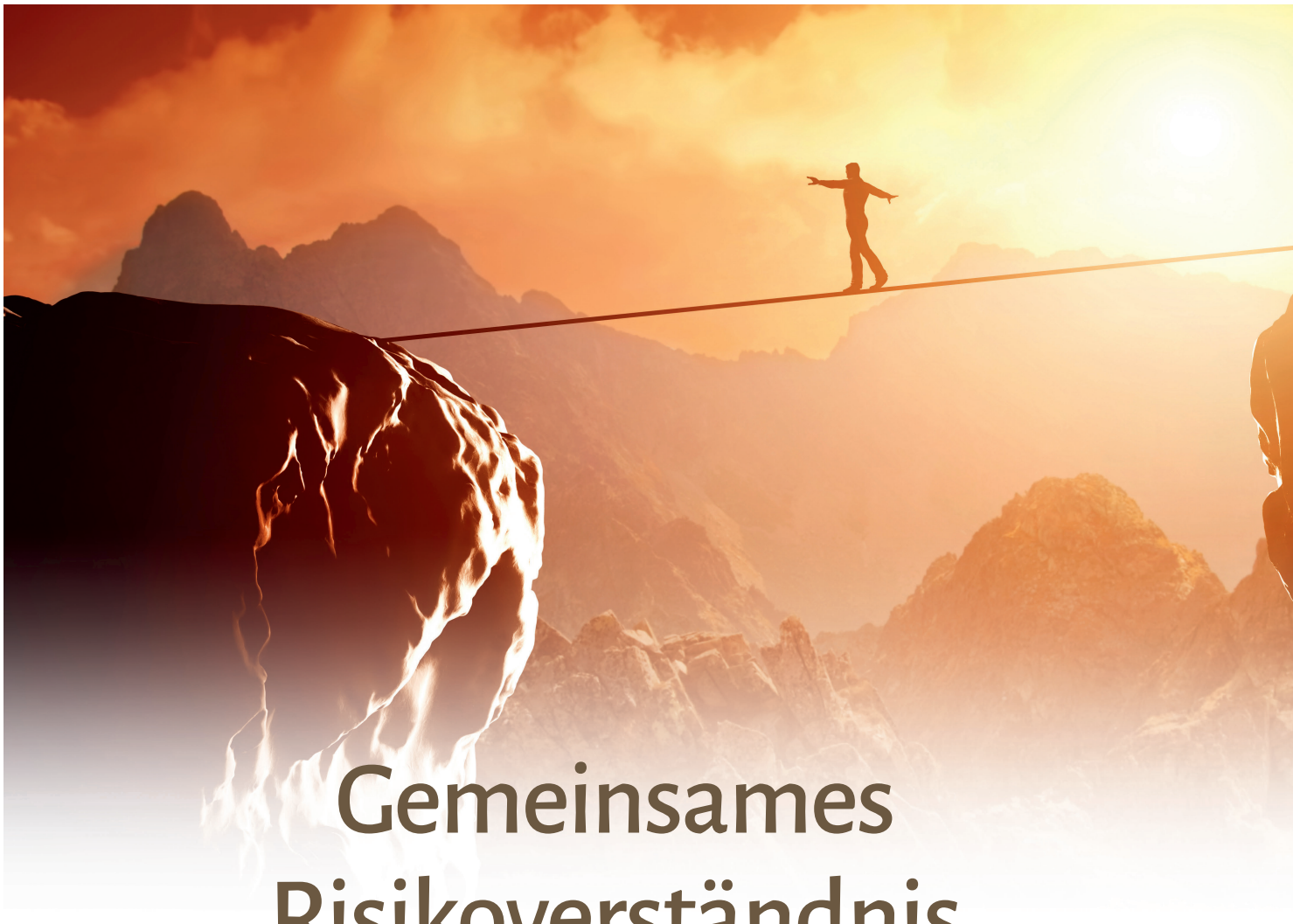

Gemeinsames Risikoverständnis

Die Bedeutung der ISO-Normen

Durch die Corona-Pandemie ist die Frage, wie Organisationen mit Risiken umgehen, verstärkt in den Blickpunkt gerückt. Dieser Beitrag gibt Hinweise auf die Notwendigkeit eines vergleichbaren Verständnisses von „Risiko" durch die verschiedenen Funktionen in Organisationen. Der Artikel zeigt außerdem auf, wie sich relevante Risiken ermitteln lassen und mit welchen Ansätzen sie „gemanagt" werden können.

Thomas Votsmeier

Am Anfang steht die Frage, welche Arten von Risiken für Organisationen und Funktionen relevant sind? Hierbei gilt es zu unterscheiden, ob man den Umgang mit Risiken aus der Perspektive einzelner Funktionsbereiche, aus der übergeordneten Perspektive für die Gesamtorganisation oder aus der Managementsystemperspektive betrachtet.

Verschiedene Risikoarten

Besonders in Hinblick auf den letzten Punkt ist es interessant, dass verschiedene ISO-Normen und Empfehlungen erarbeitet wurden, die den Umgang mit Risiken im Zusammenhang mit Managementsystemen betreffen. Ganz gleich, welche Perspektive man letztlich wählt, wichtig ist hierbei, dass alle Beteiligten dieselbe Sicht auf den Begriff „Risiko" haben. Aber ist dem auch immer so oder welche Unterschiede im Verständnis lassen sich erkennen? Betrachten wir einmal beispielhaft einige ausgewählte Funktionsbereiche und deren mögliche Sensibilisierung für „Risiken".

Die Geschäftsführung fokussiert sich beispielsweise auf Risiken hinsichtlich der wirtschaftlichen Entwicklung und Errei-

chung der Unternehmensziele. Dazu gehören unter anderem Betriebsunterbrechung, Lieferkettensicherheit, Haftung, Sicherstellung von Compliance und Forderungsausfälle. Damit zusammenhängende Risiken gilt es zu vermeiden oder zumindest zu minimieren.

Der Qualitätsbeauftragte kümmert sich um qualitätsrelevante Risiken. Dies betrifft insbesondere produkt- und prozessbezogene Risiken zur Sicherstellung der Qualitätsfähigkeit und der Kundenzufriedenheit.

Der Umweltbeauftragte beschäftigt sich primär mit Umweltaspekten und Umweltrisiken, die aus den Aktivitäten der Organisation entstehen können. Die Sicherheitsfachkraft widmet sich den Risiken hinsichtlich der Gesundheit der Mitarbeiter bei der Arbeit unter anderem auf Basis von Gefährdungsanalysen. So hat jede Funktion spezifische Risiken im Blick, die aus ihrer Sicht relevant sind oder werden können.

„Risiko" aus Sicht von ISO-Normen

Doch wie sieht es mit dem Verständnis dessen aus, was unter „Risiko" gemeint ist. Wie ist Risiko in ISO-Normen und -Regeln definiert? In den aktuellen ISO-Managementsystem-Anforderungsnormen wird Risiko definiert als „Auswirkung von Unsicherheit" (basierend auf der bisherigen Definition in Annex SL ‚Appendix 2) der ISO Directives). Die Auswirkung von Unsicherheit kann so verstanden werden, dass bestimmte Sachverhalte oder Ursachen Unsicherheit erzeugen, die Auswirkungen haben auf Ziele oder Ergebnisse der Organisation. Diese können wiederum negativ oder positiv bewertet werden.

Der Leitfaden zum Risikomanagement ISO 31000-2018 ergänzt die Risiko-Definition um „Auswirkung von Unsicherheit auf Ziele" und merkt dazu an: „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. […] Ziele können verschiedene Aspekte und Kategorien umfassen und auf verschiedenen Ebenen angewendet werden […]. Das Risiko wird üblicherweise anhand der Risikoursachen, der potenziellen Ereignisse, ihrer Auswirkung und ihrer Wahrscheinlichkeit dargestellt."

In anderen Normen werden „Risiken und Chancen" adressiert, ohne dass „Chancen" definiert werden. Managementsystemnormen beschreiben darüber hinaus Konzepte mit Risikorelevanz.

ISO 9001 nennt beispielsweise die Konzepte risikobasierter Ansatz und risikobasiertes Denken: „ISO 9001-2015 Einleitung 0.3.3 Risikobasiertes Denken: Risikobasiertes Denken ist zum Erreichen eines wirksamen Qualitätsmanagementsystems unerlässlich […]. Die Erfüllung der Anforderungen dieser Internationalen Norm verlangt von der Organisation, dass sie Maßnahmen plant und umsetzt, mit denen Risiken und Chancen behandelt werden. Die Behandlung von sowohl Risiken als auch Chancen bildet eine Grundlage für die Steigerung der Wirksamkeit des Qualitätsmanagementsystems, für das Erreichen verbesserter Ergebnisse und für das Vermeiden von negativen Auswirkungen."

„ISO 9001-2015 Anhang A.4 Risikobasiertes Denken: Diese Internationale Norm legt Anforderungen an die Organisation fest, dass sie ihren Kontext versteht und die Risiken als Grundlage zur Planung bestimmt. Dies verkörpert die Anwendung des risikobasierten Denkens bei der Planung und Verwirklichung von Prozessen des Qualitätsmanagementsystems […]. Obwohl […] festgelegt ist, dass die Organisation Maßnahmen zur Behandlung von Risiken planen muss, sind keine formellen Methoden für das Risikomanagement oder ein dokumentierter Risikomanagementprozess erforderlich[…]".

Hier setzt ISO 9001 einerseits am Prozessgedanken an und schlägt andererseits eine Brücke zum „Risikomanagement", ohne detaillierter auf eine konkrete Vorgehensweise einzugehen.

Risiken der Organisation managen

Wechselt man die Betrachtungsebene von der Sichtweise der Managementteilsysteme (QM, UM etc.) auf die Ebene der Gesamtorganisation, stellt sich die Frage, wie die Organisationsrisiken grundsätzlich und übergeordnet gehandhabt werden sollten.

Hier liegt bei der Leitung die Verantwortung für die Handhabung der Risiken der Organisation. Ein organisationsweites Risikomanagement einzuführen, ist eine sinnvolle und je nach Branche auch gesetzlich geforderte Aktivität.

Als „Risikomanagement" definiert die entsprechende Managementsystemnorm ISO 31000-2018 „koordinierte Aktivitäten zur Lenkung und Steuerung einer Organisation in Bezug auf Risiken".

Der Zweck des Risikomanagements liegt in der Schaffung und dem Schutz von Werten – durch Handhabung von Risiken, Treffen von Entscheidungen, Erstellen von Vision, Mission und Strategie, Zielerreichung und Verbesserung der Performance. Diese Grundsätze und Leitlinien sind dabei unter anderem sinnvollerweise zu beachten (Quelle: verkürzt nach ISO 31000-2018):

- Risikomanagement ist integraler Bestandteil aller Aktivitäten einer Organisation.
- Der Risikomanagementprozess soll in Strukturen, Abläufe und relevante Organisationsprozesse integriert und angewendet werden.
- Risikomanagement ist maßgeschneidert an Kontext und Ziele der Organisation.
- Risiken können auftreten, sich verändern oder verschwinden, wenn sich der Kontext einer Organisation verändert – Risikomanagement behandelt systematisch den Umgang mit Veränderungen und Ereignissen. »»

- Jeder ist für Risikomanagement mitverantwortlich.
- Der Ablauf der Risikobeurteilung sollte folgende Schritte umfassen: Risikoidentifikation, Risikoanalyse und -bewertung, Risikobehandlung.

Welche Risiken sind relevant?

Um die Relevanz von Risiken für spezifische Organisationen zu ermitteln, ist es sinnvoll, eine Kontextanalyse durchzuführen. Dies wird bereits in den Teilmanagementsystemen gefordert – hier ist sie jedoch umfassender. Die Kontextanalyse dient dazu, interne und externe Risiken zu untersuchen und zu verstehen. ISO 31000 Abschnitt 5.4 führt unter anderem folgende Sachverhalte an, die dabei adressiert werden können:

Externer Kontext

- soziale, kulturelle, politische, rechtliche, behördliche, finanzielle, technologische, wirtschaftliche und umweltbezogene Faktoren internationaler, nationaler, regionaler oder lokaler Art;
- für die Organisationziele maßgebliche Schlüsselfaktoren und Trends;
- Beziehungen, Wahrnehmung, Werte, Bedürfnisse und Erwartungen externer Stakeholder;
- vertragliche Regeln;
- Netzwerke und Abhängigkeiten.

Interner Kontext

- Kultur, Vision, Mission, Werte;
- Leitung, Organisationsstruktur, Rollen und Rechenschaftspflichten;
- Strategie, Ziele und Grundsätze;
- angewandte Normen, Leitlinien und Modelle;
- Kompetenzen und Ressourcen;
- Daten, Informationssysteme und Informationsflüsse;
- Beziehungen zu internen Stakeholdern;
- vertragliche Bindungen;
- gegenseitige Abhängigkeiten und Verbindungen.

Wie unschwer zu erkennen ist, handelt es sich dabei um eine umfängliche Betrachtung aller potenziellen Umfeldrisiken, die über einen generischen Risikomanagementprozess adressiert werden sollten (die Beschreibung einer sinnvollen Vorgehensweise findet sich in ISO 31000-2018).

Umsetzung in der Organisation

Wie lässt sich der Risikomanagementansatz einer Organisation umsetzen und in das vorhandene Managementsystem integrieren? Da sich Risiken auf allen Ebenen der Organisation ergeben, ist es sinnvoll, die Frage der Risikoermittlung und -behandlung in alle relevanten Prozesse der Organisation zu integrieren.

So kann jeder Prozessverantwortliche diese Aspekte in den Prozessablauf aufnehmen, bewerten und nachvollziehbar dokumentieren. Relevant sind dabei die Informationen oder Kenntnisse, die durch Auftreten von Unsicherheiten die Zielerreichung oder das Ergebnis des Prozesses gefährden können.

Hinweis: Wie die Vorgehensweise von Risikomanagement nach ISO 31000 in Managementsysteme auf Basis von Normen, die der High Level Structure folgen, integriert werden kann, wird im kürzlich erschienenen „ISO IWA 31:2020-03 Risk management – Guidelines on using ISO 31000 in management systems“ dargelegt. Dort wird erläutert, wie die Abschnitte der ISO 31000 in Bezug stehen zu den Abschnitten mit Anforderungen aus der „High level structur (HLS) for Management Systems“.

Unter Zuhilfenahme der genannten Normen, Leitfäden und Veröffentlichungen von ISO lassen sich ein gemeinsames Verständnis herstellen und strukturierte Vorgehensweisen zur Risikobeurteilung abstimmen.

Organisationsweites Risikomanagement ist sinnvoll

Zum Schutz und Erhalt der Werte einer Organisation ist ein umfassendes organisationsweites Risikomanagement sinnvoll und zielführend. Als Leitfaden für eine wirksame Umsetzung kann der Risikomanagementansatz nach ISO 31000 dienen. Um aktuell zu bleiben und alle relevanten Personen und Funktionen einzubinden, ist die Integration der Risikobehandlung in die Organisationsprozesse ein bedeutender Faktor. Dies berücksichtigen die entsprechenden Managementsystemnormen auch über den „risikobasierten Ansatz“.

Der Einsatz von für die jeweilige Organisation passenden Tools zur Risikoermittlung,-bewertung und -behandlung unterstützt die Akzeptanz und Wirksamkeit des gewählten Vorgehens. ■

INFORMATION & SERVICE

LITERATUR

DIN EN ISO 9000:2015-11. Qualitätsmanagementsysteme – Grundlagen und Begriffe (ISO 9000:2015). Beuth, Berlin
DIN EN ISO 9001:2015-11. Qualitätsmanagementsysteme – Anforderungen (ISO 9001:2015). Beuth, Berlin
DIN ISO 31000:2018-10. Risikomanagement – Leitlinien (ISO 31000:2018).Beuth, Berlin
ISO IWA 31:2020-03. Risk management – Guidelines on using ISO 31000 in management systems
ISO/IEC Directives, Part 1. Consolidated ISO Supplement – Procedures specific to ISO. (10th edition). International Organization for Standardization, Geneva
Herdmann. Frank: Drei Schritte zum effektiven und effizienten Risikomanagement nach DIN ISO 31000. Beuth, Berlin 1. Auflage 2018.

AUTOR

Thomas Votsmeier ist Leiter Normung/Internationale Kooperationen bei der Deutschen Gesellschaft für Qualität..

KONTAKT

T +49 69 95424–145
thomas.votsmeier@dgq.de