ISO 31000 versus ISO 14971:

Sinnvolle Schnittstellenbildung trotz Differenzen?

Jennifer Siemers, Dr. Christian Wicenec, Prof. Dr. Jana Wolf

Lücken schliessen, Reputationsschäden vermeiden, Patienten und Anwender schützen: Ziele des Medizinprodukterisikomanagements.

In der Medizintechnikbranche ist die präventive Bewältigung von Produktqualitätsrisiken schon aufgrund möglicher Gefährdungen von Anwendern und Patienten von zentraler Bedeutung. Dabei sind die qualitätsorientierte Prozessoptimierung sowie die präventive Minderung produktimmanenter Risiken ebenso gängige Massnahmen, wie die ständige Beobachtung der auf dem Markt befindlichen Produkte auf Basis eines vorab geplanten Überwachungsprozesses, um mögliche Eskalations- und Schadenspotenziale zu beherrschen. Die Folgen eines Produktqualitätsrisikos reichen jedoch weiter:

Realisieren sich Risiken der Produktsicherheit oder Produktqualität, leidet neben der Kundenakzeptanz auch die Reputation eines Unternehmens, was negative Folgen für dessen wirtschaftlichen Erfolg mit sich bringt.

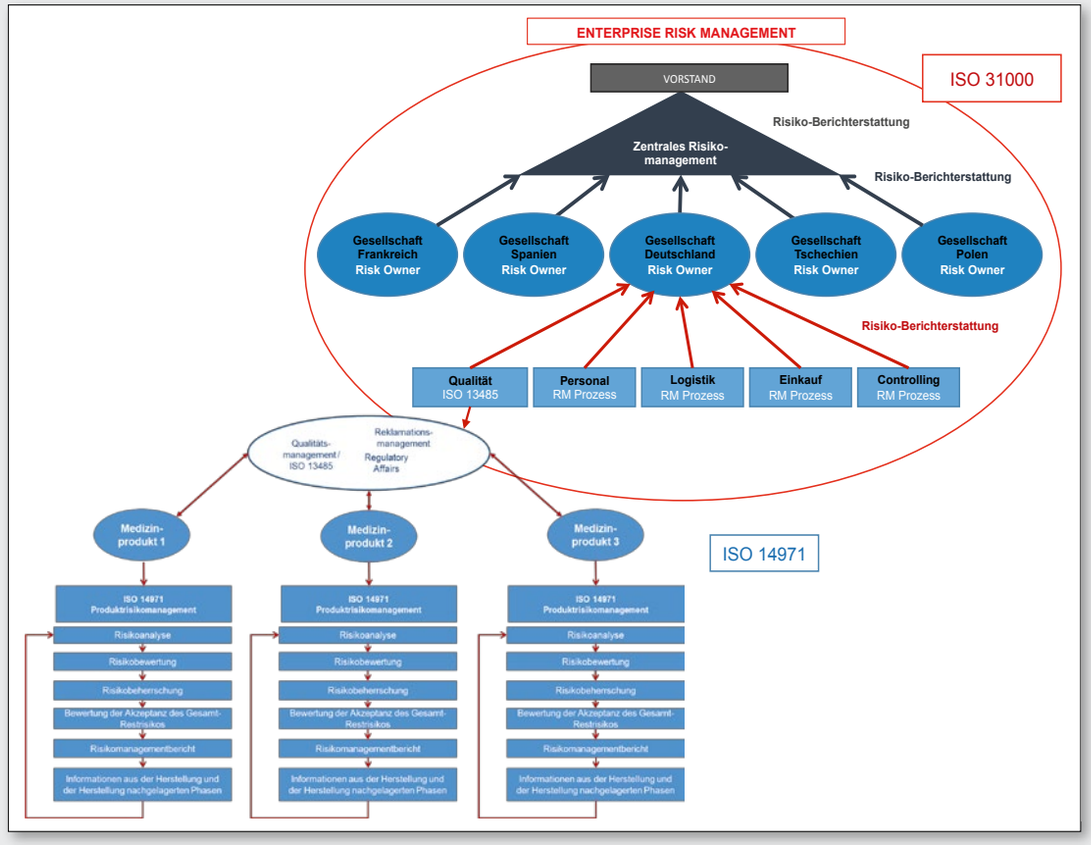
Silodenken erschwert Risikoübersicht

Obwohl sie gleichermassen unternehmensrelevant und inhaltlich miteinander verwoben sind, werden Qualitäts- und Risikothemen historisch aufgrund ihrer spezifischen regulatorischen Anforderungen oft im jeweiligen Fachressort isoliert bearbeitet. Der durch diese fachliche Isolierung möglicherweise unvollständige Informationsaustausch kann zu einer fehlerhaft eingeschätzten Risikogesamtsituation des jeweiligen Unternehmens und damit bei Entscheidungen, die auf Basis dieser Informationen gefällt werden, zu ernsthaften wirtschaftlichen Problemen führen. Eine Schnittstelle zwischen dem Produktrisikomanagement und dem Enterprise Risk Management (ERM) vermeidet eine solche problematische Berichtslücke.

Analyse der unterschiedlichen Risikomanagementsysteme als Schnittstellengrundlage

Um eine derart universelle Schnittstelle zu entwerfen, müssen zunächst die jeweiligen Systemgrundlagen analysiert werden. Hier bietet sich ein Vergleich

Abb. 1 Zusammenhang ISO 31000 und ISO 14971 im Unternehmen



Prof. Dr. Jana Wolf ist Professorin an der Hochschule Aalen, Fakultät Wirtschaftswissenschaften, Studiengang Gesundheitsmanagement. www.htw-aalen.de
Jennifer Siemers ist Bachelorandin ebenda.
Dr. Christian Wicenec ist Leiter Risk Management bei der Paul Hartmann AG (www.hartmann.de). Er betreute die Bachelorarbeit von Jennifer Siemers mit.

des Risikomanagementstandards ISO 31000, der als Anleitung zum Aufbau eines Risikomanagementsystems branchenübergreifend genutzt werden kann, mit der ISO 14971, die spezifische Anforderungen an das Risikomanagement von Medizinprodukten nach § 3 MPG stellt, an.

Ein Vergleich der Normen zeigt, dass schon ihre Verbindlichkeit voneinander abweicht. Ist die ISO 31000 als allgemeine Anleitung für die Implementierung eines ERM gedacht, so wird die ISO 14971 seitens der EU als beste Lösung zur Umsetzung der Anforderungen aus der Richtlinie 93/42/EWG betrachtet.

Unterschiedliche Ziele und Anwendungsbereiche

Auch Ziel und Anwendung der Normen unterscheiden sich. Während die ISO 31000 den Schutz von Vermögenswerten zum Ziel hat, ist die ISO 14971 als Werkzeug auf die Vermeidung von produktinduzierten Schäden an Anwendern, Patienten, Gegenständen und Umwelt ausgerichtet. Die ISO 31000 beschreibt Anforderungen an ein erfolgreiches ERM, die Norm wird für Unternehmensfunktionen und alle denkbaren Risikoarten im internen und externen Kontext angewendet. Sie befasst sich mit grundsätzlichen Zielen zur Erfüllung von Kundenbedürfnissen, mit Produkten, Dienstleistungen, wichtigen Märkten, Zielkunden, sowie den dafür benötigten Fähigkeiten und Ressourcen. Dagegen fokussiert die ISO 14971 auf die Produkteigenschaften und die Prozesse des gesamten Produktlebenszyklus und betrachtet somit ausschliesslich produktorientiert Risiken, wie Risiken des Produktdesigns oder die Prozessrisiken des Produktlebenszyklus.

Differente Integrationspotenziale

Aufgrund der unterschiedlichen Fokussierung auf unternehmensbezogene und produktbezogene Themen, ergeben sich auch eine unterschiedliche Integrationstiefe und unterschiedliche Integrationspotenziale. Während die ISO 31000 als System nach dem Top-Down-Prinzip die ganze Organisation von oben nach unten durchdringen soll, entspricht die ISO 14971 als operativer Prozess dem Bottom-Up-

Unterschiede zwischen dem monetären, unternehmensbezogenen Standard ISO 31000 und den gesundheitsgefährdenden, produktbezogenen Anforderungen der ISO 14971 existieren.

Prinzip. Die Integration des Produktrisikomanagements in das Qualitätsmanagement ist nach Empfehlung der ISO 13485, bei Medizinprodukteherstellern sinnvoll. Dagegen soll das ERM andere Systeme zur umfassenden Risikobewältigung zumindest durch Schnittstellen anbinden, wenn nicht sogar integrieren. Auch wird im ERM eine zentral koordinierende Abteilung empfohlen, die die Rahmenbedingungen, Methoden und Werkzeuge des Risikomanagements festlegt und die Risikoverantwortlichen bei der operativen Ausführung des Risikomanagementprozesses unterstützt. *(Abbildung 1)* Dabei müssen jedoch alle am Risikomanagement Beteiligten individuell den gesamten Risikomanagementprozess durchlaufen. Das Produktrisikomanagement ist dagegen organisatorisch nicht als Abteilung vorgesehen, sondern als Prozess innerhalb von Projekten gedacht. Je nach Prozessschritt und Produkt wechselt die Verantwort-

Abb. 2 Vergleich der Normen

Vergleich ISO 31000 und ISO 14971

	ISO 31000/ Enterprise Risk Management	ISO 14971/ Produktrisikomanagement
Anwendungsbereich	Branchenunabhängig	Hersteller von Medizinprodukten
Ziel	Schutz Bestand des Unternehmens	Schutz Patienten, Anwender, Umwelt
Gesetzlicher Hintergrund	Gefordert in KonTraG und BilMoG, kann verschieden eingehalten werden	Gefordert in 93/42/EWG, ISO 14971 wird als beste Möglichkeit zur Einhaltung betrachtet
Organisation	Zentral, dezentral, beides	Dezentral, nach Produktgruppe
Einordnung in das Unternehmen	Strategisch und operativ	Operativ
Integration	Als Abteilung bis hin zu Managementsystem	Prozess innerhalb eines Projektes, kann in Qualitätsmanagement integriert werden
Verantwortung	Verantwortung nach Bereich	Verantwortung nach Produkt und Prozessschritt
Risikomanagementprozess	Regelmäßige Wiederholung, mindestens jährlich	Vergrößerte Zeitabstände, wenn keine Veränderungen
Bewertung	Quantitativ, Geldeinheit	Halb-quantitativ, Häufigkeiten
Externe Berichterstattung	Jährlich	Nur bei medizinisch relevanten Vorkommnissen
Orientierung	Lebenszyklus des Unternehmens	Lebenszyklus des Produktes

lichkeit von einer Unternehmensfunktion zur anderen.

Empfehlung vs. Vorgabe des Risikomanagement-prozesses

Die Analyse der jeweiligen Risikomanagementprozesse zeigt in vielen Prozessschritten Unterschiede. So gibt die ISO 31000 bei der Risikoidentifikation keine spezifische Methode vor, sondern listet stattdessen gängige Methoden in der ISO 31010 auf. Demgegenüber schreibt die ISO 14971 unter anderem gezielt die Fehlermöglichkeits- und Einflussanalyse oder die modifizierte Fehlerbaumanalyse vor. Auch ist die Risikoanalyse in den Normen unterschiedlich definiert. In der ISO 31000 sind dies die Beschreibung des Risikos und dessen Ursachen. Dagegen wird in der ISO 14971 die Einschätzung jedes Risikos für jede Gefährdungssituation als Risikoanalyse verstanden.

Unterschiedliche Methoden der Risikobewertung

Unterschiede zeigen sich auch im Prozessschritt der Bewertung identifizierter und analysierter Risiken. Im ERM wird die quantitative Bewertung bevorzugt. Berechnet werden potenzielle finanzielle Verlustwerte, die in Relation zu Planwerten gestellt werden. Im Produktrisikomanagement wird stattdessen eine anteilig qualitative Scoring-Methode gewählt, bei der aus der Auftrittswahrscheinlichkeit, des möglichen Schadensausmasses und der Entdeckungswahrscheinlichkeit eine Risikoprioritätszahl berechnet wird.

Massnahmen zwischen Auswahl und Determination

Zur Risikobewältigung müssen Massnahmen ausgewählt und beurteilt werden. Die ISO 31000 gibt dabei keine Bewältigungsmassnahmen vor. Der Risikomanager kann zwischen verschiedenen Mitigationswegen wählen. Dagegen determiniert die ISO 14971 mögliche Massnahmen zur Minderung der Risiken, wie zum Beispiel integrierte Designsicherheit. Eine Überprüfung der Massnahmenwirksamkeit ist in beiden Normen Pflicht. Effizienzbetrachtungen erfolgen jedoch ebenfalls unterschiedlich. Die ISO 31000 vergleicht Massnahmenkosten mit dem Nutzen aus dem Nichteintreten des Risikos, die ISO 14971 vergleicht den medizinischen Nutzen für den Patienten, unter den verschiedensten Aspekten wie Recht, Politik, Ökonomie oder Technik, mit dem Risiko der Produktanwendung.

Feste Intervalle und situationsbedingter Aktionen

Auch die Gegenüberstellung des Prozess- und Berichterstattungsturnus der Normen ist wichtig. Während die ISO 31000 – ausserhalb dringender Ad-hoc-Risikomeldungen – regelmässige Intervalle der Risikoidentifikation und -überprüfung nahelegt, erfolgt der Produktrisikomanagementprozess anlassbezogen, wenn z. B. durch Beobachtung des Marktes oder der Gesetzgebung die Notwendigkeit einer Veränderung des Produktes besteht. Aufgrund gesetzlicher Vorgaben zum Lagebericht (DRS 20) erfolgt die externe Berichterstattung des ERMs regelmässig im Chancen- und Risikobericht des Lageberichtes. Das Produktrisikomanagement berichtet dagegen nur extern über (realisierte) Produktrisiken, wenn die Meldung eines Vorkommnisses an die für Medizinprodukte zuständige Behörde (BfArM) erforderlich wird. Eine kontinuierliche Verbesserung des ERM erfolgt nach ISO 31000 prozessorientiert, bei der ISO 14971 jedoch produktorientiert.

Schnittstelle trotz aller Unterschiede sinnvoll

Der Vergleich der beiden Normen zeigt Differenzen. Dennoch besteht aufgrund der Generik der ISO 31000 Raum für eine Schnittstelle zwischen dem darin beschriebenen ERM und dem Produktrisikomanagement nach ISO 14971. Diese besteht vor allem im Austausch von Risikoinformationen aus dem Produktrisikomanagement, die zusätzlich monetär bewertet werden. Lücken in der Risikoidentifikation können so geschlossen und unternehmensübergreifende Massnahmen gezielter und frühzeitiger durchgeführt werden. ■

Begriffsdefinitionen (Orientierung von ISO 31000 und ISO 14971)

Speziell auch in den Begriffsdefinitionen spiegelt sich die Unterschiedlichkeit der Normen wieder. Zum Beispiel wird der Begriff «Risiko» in den ISO-Normen in Abhängigkeit ihrer Betrachtungsweise definiert und charakterisiert. Auch der Begriff «Schaden» bedeutet in den Normen nicht das Gleiche:

Nach ISO 31000 wird dieser als wirtschaftlicher Verlust für das Unternehmen verstanden und nicht wie in der ISO 14971 als Verletzung der menschlichen Gesundheit oder Gefährdung der Umwelt. Deshalb geht mit der Begriffsdefinition eine eigentliche Konnotation der Risikobeherrschung einher. Nach ISO 14971 ist ein Risiko beherrschbar, diese Sichtweise existiert in der ISO 31000 nicht.