Schluss mit Wohlfühl-Risikomanagement !

Prof. Dr. Bruno Brühwiler

Netzwerk Risikomanagement 27. März 2019

Ausgangslage für Weiterentwicklung der Risikomanagement-Normen

- Revision der ISO 31000
- Bedürfnis nach Spezifikation von deren Inhalten
- Erfolgsgeschichte der 49000-Serie, vor allem in der Ausbildung von klinischen Risikomanagern
- Weiterentwicklung von Managementsystemen, insbesondere auch die ISO High Level Structure
- Kontinuierliche Verbesserung durch Aktualisierung mit den Erfahrungen in der Ausbildung und Beratung
- Anforderung: Hoher Wiedererkennungswert durch Beibehaltung von Struktur und z.B. Prozess RM

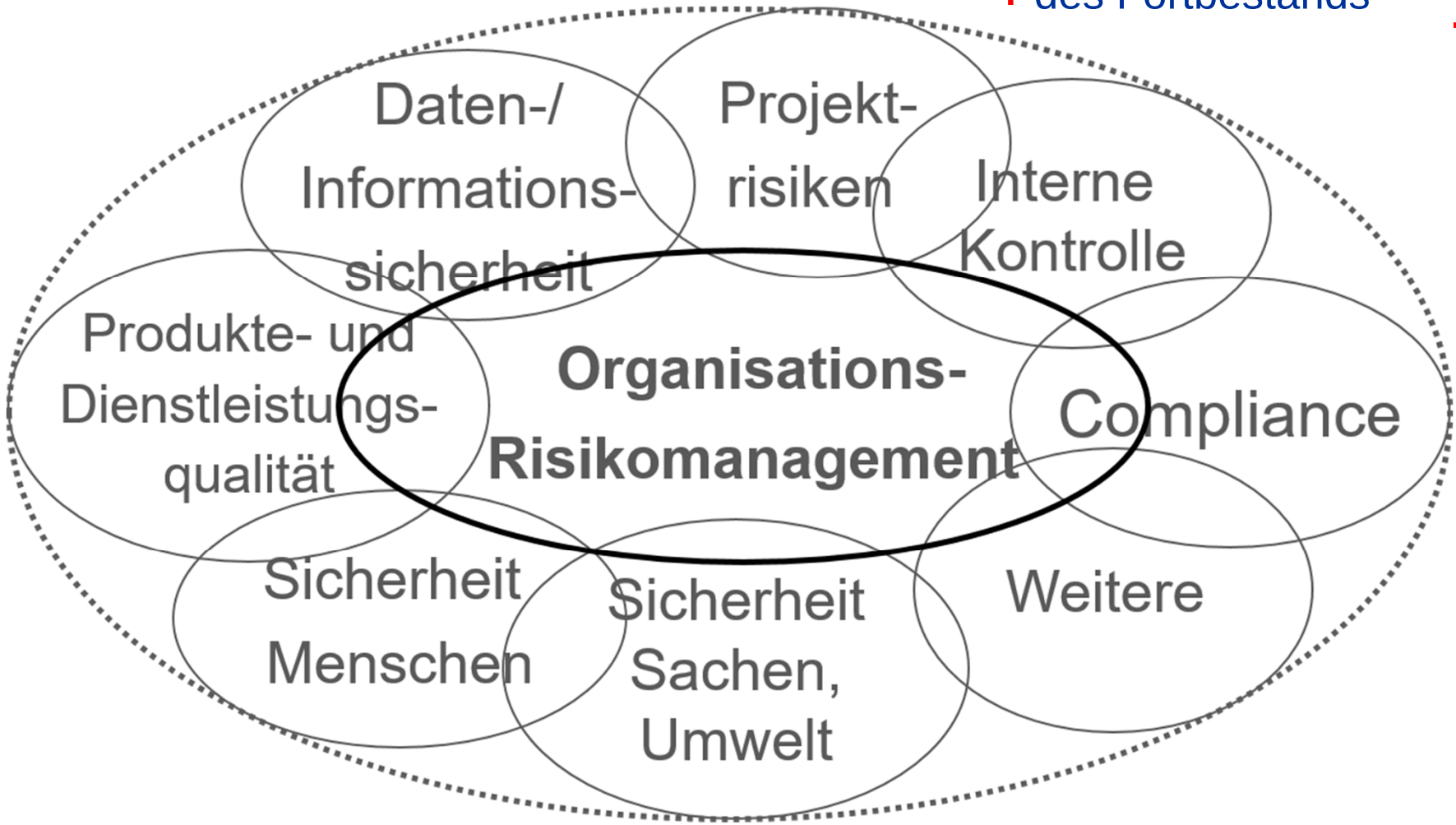
Umfang des Risikomanagement-Systems

„Das Risikomanagement-System erstreckt sich nicht nur auf das Organisations-Risikomanagement, in welchem sich die oberste Leitung mit den bestandsgefährdenden Risiken befasst.

Es erstreckt sich auch auf die auf dem risikobasierten Ansatz aufgebauten Teilbereiche wie Produkt- und Dienstleistungsqualität, Sicherheit für Menschen, Sachen und die Umwelt, interne Kontrollsysteme, Compliance, Datenschutz und Informationssicherheit, Projekt-Risiken und weitere risikobasierte Anwendungsbereiche“.

Das Grundkonzept in einem integrierten Managementsystem

Ziel ist die Sicherung des Fortbestands



Einschluss des Notfall-, Krisen- und Kontinuitätsmanagements

Der Risikomanagement-Prozess muss umfassen:

- die Früherkennung von Risiken (Bedrohungen, Chancen)
- die Analyse und Bewertung der Risiken,
- die Frühwarnung bei drohendem Schaden,
- die Bewältigung und Überwachung von Risiken,
- die Reaktion auf plötzlich eintretende Schadenereignisse und
- die Erkennung und Wahrnehmung von Chancen zur Organisationsentwicklung.

Zwei zentrale Fragen der Weiterentwicklung:

Bei der Weiterentwicklung eines Normenwerkes wird immer eine Arbeitsgruppe benötigt, um die Meinungen / Konzepte breit abzustützen.

Die Arbeitsgruppe besteht aus ausgewiesenen Experten von Österreich, Deutschland und der Schweiz, Personen mit Erfahrungen und Interessen im Risikomanagement.

Frage 1: Wollen wir die HLS konsequent umsetzen?

Frage 2: Wollen wir eine zertifizierbare Norm schaffen?

Beide Fragen wurden mehrheitlich mit Ja beantwortet.

Merkmale der Zertifizierung

Um eine Norm zertifizieren zu können, braucht es «MUSS»-Anforderungen. Dies bedeutet konkret, dass solche Anforderungen eindeutig überprüfbar sind, damit festgestellt werden kann, ob eine Organisation die Anforderungen der Norm auch wirklich erfüllt.

Bisher war die ONR 49000-Serie nur andeutungsweise auf eine Zertifizierung ausgerichtet. Dies führte dazu, dass in der ONR 49001 viele erklärende Texte und Ausführungen enthielten.

In der neuen ÖNORM 4901 wird auf Erklärungen und Erläuterungen verzichtet und entweder in die ÖNORM 4900 oder in die Leitfäden transferiert. Die zertifizierbare ÖNORM 4901 enthält nur noch Anforderungen und wenige Anmerkungen. Sie ist deshalb prägnanter und verbindlich formuliert und auch kürzer als die bisherige ONR.

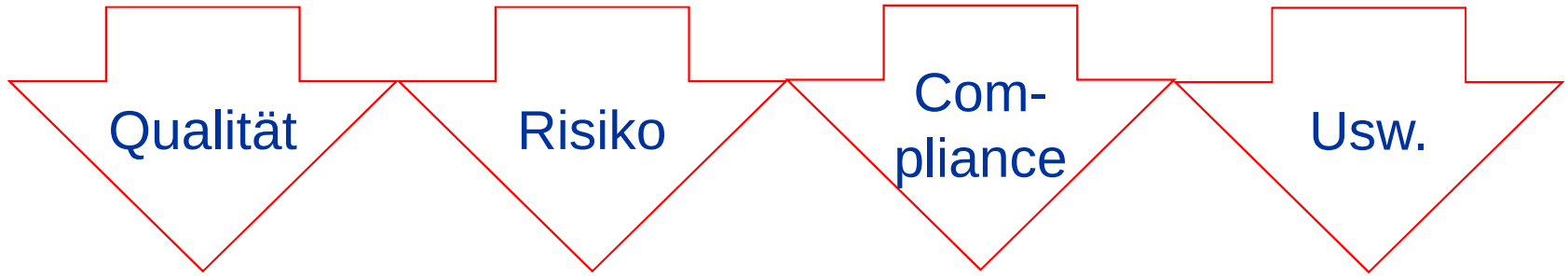
Zertifizierung – was bedeutet das?

- Die Anforderungen der Norm werden in den wesentlichen Punkten erfüllt,
- die **Wirksamkeit** des Risikomanagements ist gegeben, wenn die Anforderungen der Norm angemessen an die Bedürfnisse der Organisation massgeschneidert erfüllt werden,
- unabhängige Experten können bestätigen, ob die Anforderungen der Norm erfüllt werden,
- absolute Sicherheit kann durch eine Zertifizierung nicht garantiert werden, Restrisiken bestehen immer.

Die ISO Management-System-Struktur dient der Integration von Risikomanagement in ISO- Managementsysteme

1. Anwendungsbereich
2. Normative Verweisungen
3. Begriffe
4. Kontext der Organisation
5. Risikomanagement als Führungsaufgabe
6. Planung des Risikomanagement-Systems
7. Unterstützung des Risikomanagements
8. Betrieb des Risikomanagement-Prozesses
9. Bewertung der Wirksamkeit des Risikomanagement-Systems
10. Verbesserung des Risikomanagement-Systems

Integration von verschiedenen Managementsystemen wird direkt unterstützt



ISO Management-System-Struktur

«Doppelspurigkeiten sind zu vermeiden»

Anwendungsbereich gewährleistet die Wirksamkeit des Risikomanagements

Die Organisation muss die organisatorischen Grenzen und die inhaltliche Anwendbarkeit ihres Risikomanagement-Systems bestimmen, um dessen Anwendungsbereich festzulegen.

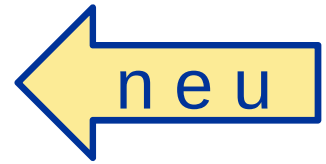
Dabei muss die Organisation

- den internen und externen Kontext,
- die Erwartungen und Anforderungen der interessierten Parteien,
- die strategischen Ziele, operativen Tätigkeiten und bindende Verpflichtungen und
- die Bereiche des Organisations-Risikomanagements und der risikobasierten Ansätze beachten.

Dabei ist sicherzustellen, dass die wesentlichen Risiken berücksichtigt werden.

Die Wirksamkeit wird durch die Rollen und Verantwortlichkeiten im Risikomanagement gesichert

- Oberste Leitung und Überwachungsorgane
- Risikoeigner
- Risikomanager
- Auditoren / Revisoren



Führung und Verpflichtung der obersten Leitung

Die oberste Leitung muss sicherstellen, dass das Risikomanagement gemäss dem Anwendungsbereich in die Organisation eingebunden wird, indem sie

a. die Rechenschaftspflicht für das Risikomanagement-Systems übernimmt,
b. die Komponenten des Risikomanagement-Systems angemessen gestaltet, umsetzt, bewertet, laufend verbessert und weiterentwickelt,
c. eine Risikopolitik erlässt und eine Vorgehensweise festlegt, welche dem Kontext der Organisation, ihren Zielen, Tätigkeiten und Anforderungen entspricht,
d. die Risikotragfähigkeit der Organisation angemessen festlegt,
e. sicherstellt, dass die notwendigen Ressourcen dem Risikomanagement zugeteilt werden,
f. die Befugnisse und Verantwortung den entsprechenden Stufen in der Organisation zuweist,
g. die bedeutendsten Risiken der Organisation regelmäßig in den dafür verantwortlichen Gremien behandelt und steuert und
h. die Überwachungsorgane, falls solche gegeben sind, in das Risikomanagement angemessen einbezieht.

Risikoeigner und Risikomanager sind für die Umsetzung in der zentralen Verantwortung

Risikoeigner:
Person mit der Entscheidungskompetenz und Verantwortung, hinsichtlich eines Risikos zu handeln.

Risikomanager:
Der Risikomanager kann den Risikomanagement-Prozess anwenden und in Organisationen umsetzen.

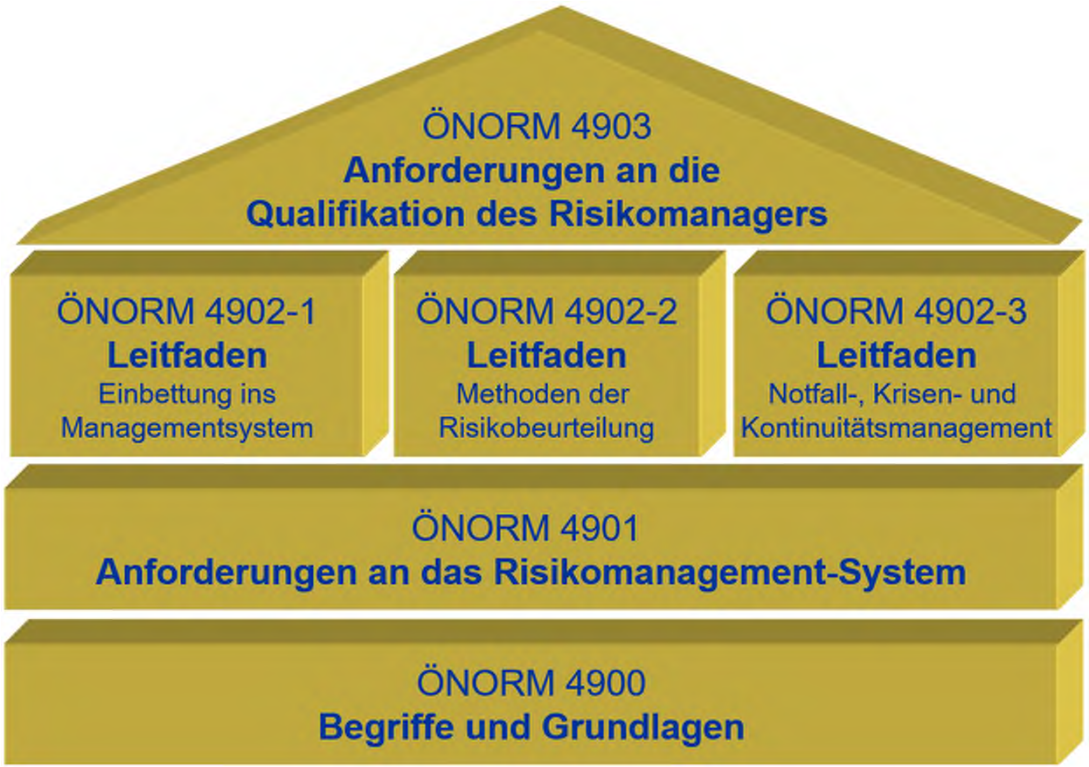
Auditoren bzw. Revisoren stellen die Wirksamkeit des Risikomanagements fest

Die Auditoren bzw. Revisoren müssen prüfen, wieweit die Anforderungen an das Risikomanagement von der Organisation erfüllt werden.

ANMERKUNG 1 Grundsätze der Führung, Satzungen oder Entscheidungen können festlegen, dass Auditoren und/oder Revisoren die Wirksamkeit des Risikomanagements in objektiver und unabhängiger Art prüfen und die Ergebnisse der obersten Leitung bzw. den Überwachungsorganen berichten müssen. Es kann sich dabei um interne Personen und Organe handeln oder um externe Personen bzw. Organisationen.

ANMERKUNG 2 Externe Auditoren von dazu autorisierten Zertifizierungs-stellen können Konformitätsprüfungen bzw. ein externes Audit mit anerkannter Zertifizierung durchführen.

Weiteres Vorgehen – Zeitplan



Abschluss 2. Q. 2019
Verfügbar 3. Q. 2019

Abschluss 1. Q. 2019
Verfügbar 2. Q. 2019

Ausblick: Nicht mehr unverbindliche Empfehlungen, sondern überprüfbare Anforderung

ISO 31000 und die bisherige Spezifikation mit der ONR 49000 sind Empfehlungen mit vielen erläuternden Beschreibungen und Erklärungen, worum es beim Risikomanagement geht.

Die «neue Welt» der ÖNORM 4901 besteht aus Anforderungen, die verbindlich formuliert und damit konkret überprüfbar sind. Die Zeit des Wohlfühl-Risikomanagements geht zu Ende.